RGPD 2018

ENJEUX ET CONSÉQUENCES POUR LES PROFESSIONNELS DE SANTÉ

LIVRE BLANC

versushealth Architecte numérique e-santé

Les enjeux du Règlement Général de Protection des Données (RGPD)

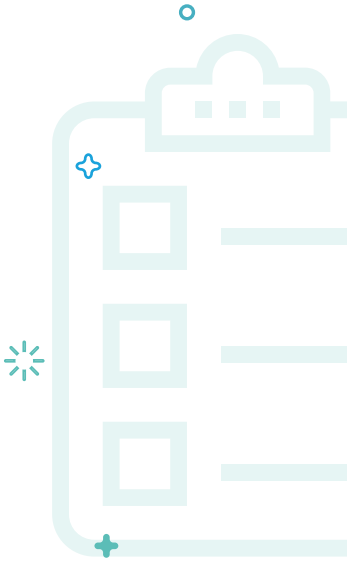
Soucieuses de la protection des données personnelles des personnes physiques, les institutions européennes ont décidé en décembre 2015 d'un "Règlement Général de Protection des Données" ou RGPD qui entrera en vigueur le 25 mai 2018. Ce nouveau cadre réglementaire a 3 objectifs :

1. Uniformiser la réglementation au niveau européen

2. Responsabiliser les entreprises

3. Renforcer le droit des personnes

   Droit d'information (Art 13 et 14), droit d'accès (Art 15), droit de rectification (Art 16), droit à l'effacement (Art 17), droit à la limitation (Art 18), droit à la portabilité (Art 20), prise de décision automatisée (Art 22).



Quelles sont les sanctions possibles en cas de non conformité ?

Les sanctions administratives*

Prononcer un avertissement

Mettre en demeure l'entreprise

Limiter temporairement ou définitivement un traitement

Ordonner de satisfaire aux demandes d'exercice des droits des personnes

Suspendre les flux de données

Ordonner la rectification, la limitation ou l'effacement des données

Les sanctions financières*

Elles peuvent s'élever, selon la catégorie de l'infraction, de 10 ou 20 millions d'euros, ou, dans le cas d'une entreprise, de 2% jusqu'à 4% du chiffre d'affaires annuel mondial, le montant le plus élevé étant retenu.

* Source : La CNIL

Zoom sur les données de santé

par notre expert juridique

Le RGPD est un texte exigeant en matière de protection des données personnelles, données auxquelles il offre une définition très englobante.

Dans ce contexte de généralisation de la protection des données personnelles, les données de santé ne sont en rien banalisées.

D'une part, et pour la première fois au niveau européen, un texte en donne une définition harmonisée, et par là renforce leur spécificité.

Considérant 35 Les données à caractère personnel concernant la santé devraient comprendre l'ensemble des données se rapportant à l'état de santé d'une personne concernée qui révèlent des informations sur l'état de santé physique ou mentale passé, présent ou futur de la personne concernée.

D'autre part, les données de santé sont catégorisées en tant que données sensibles, cela signifiant leur particulière vulnérabilité et leur caractère «a-commercial». Les données de santé sont strictement identifiées comme support d'une finalité médicale précise et bénéficient d'un principe général d'interdiction de traitement, sauf nécessités restrictivement définies et exclusivement avec le consentement des personnes concernées :

- Sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne physique, dans le cas où la personne concernée se trouve dans l'incapacité physique ou juridique de donner son consentement.

Médecine préventive ou médecine du travail, appréciation de la capacité de travail du travailleur, diagnostics médicaux, prise en charge sanitaire ou sociale, ou gestion des systèmes et des services de soins de santé ou de protection sociale ou en vertu d'un contrat conclu avec un professionnel de santé et soumis au secret.

Motifs d'intérêt public dans le domaine de la santé publique, tels que la protection contre les menaces transfrontalières graves pesant sur la santé ou garanties des normes élevées de qualité et de sécurité des soins de santé et des médicaments ou des dispositifs médicaux.

Recherche scientifique.

Il appartient aux opérateurs de santé de renforcer leur vigilance. La responsabilisation des individus par rapport à l'usage de leurs données personnelles, induite par le RGPD, a permis de lever la demande d'autorisation préalable à la CNIL pour les traitements tels que les dossiers médicaux partagés, les dispositifs de télémédecine ou d'éducation thérapeutique.

Pour autant, les contraintes demeurent. L'enjeu de la conformité appliquée aux données de santé est d'adopter une méthodologie qui permette une identification appropriée de la finalité de la donnée recueillie, de la durée de sa conservation, cela afin d'y adapter le bon niveau de protection.

Les professionnels de la santé vont devoir se conformer à 7 grands principes

1. Accountability

La charge de la preuve de la conformité est à la charge de l'entreprise. Cela implique de documenter tous les processus et mesures mis en œuvre.

Exemple | **Contrôle CNIL**

Lors d'un contrôle de la CNIL, il conviendra de fournir l'ensemble de la documentation démontrant la mise en conformité. Cela inclut, entre autre, la PSSI, le registre des traitements, les procédures mises en œuvre pour faire valoir les droits des personnes concernées, les méthodologies de gestion des risques, les PIA, ...

2. Principe de licéité

Les données à caractère personnel ne peuvent être recueillies et traitées que pour un usage déterminé et légitime, correspondant aux missions du responsable du traitement.

Exemple | **Fournir des données medicales**

Un établissement de santé ne pourra, par exemple, pas fournir de données médicales à des compagnies d'assurance qui en feraient un usage commercial.

3. Principe de minimisation

Seules les données strictement nécessaires à la finalité du traitement peuvent être collectées.

Exemple | **Consultation médicale**

Dans le cadre d'une consultation médicale, il n'apparaît pas nécessaire de collecter l'adresse IP d'un patient. Cette information n'ayant pas de rapport avec la finalité du traitement.

4. Principe de conservation limitée

Les données personnelles ne peuvent être conservées que le temps nécessaire à l'exécution du traitement.

Exemple | **Données personnelles**

Légalement, les dossiers médicaux doivent être conservés 10 ans. Cependant les données personnelles concernant les traitements annexes, sont soumises à cette règle. Par exemple, lors de la facturation d'un acte médical, les coordonnées bancaires du patient ne devraient stockées que le temps de la transaction.

5. Principe de sécurité

Toutes les mesures nécessaires à la sécurisation des données personnelles (confidentialité, intégrité, disponibilité) doivent être mises en place.

Exemple | **Mesure de sécurité**

Il est obligatoire de mettre certaines mesures de sécurité en œuvre afin d'éviter toute fuite ou perte de données. Cela peut inclure le cloisonnement des zones hébergeant des données sensibles, un durcissement des postes de travail, une gestion centralisée des incidents de sécurité,... Dans tous les cas l'ensemble des mesures à appliquer seront définies lors d'une analyse des risques et consignées dans une DDA (déclaration d'applicabilité).

6. Principe de security by design

La sécurité des données personnelles doit être prise en compte dès la phase de conception de toute activité (services, développement applicatif, etc.).

Exemple | **S-SDLC**

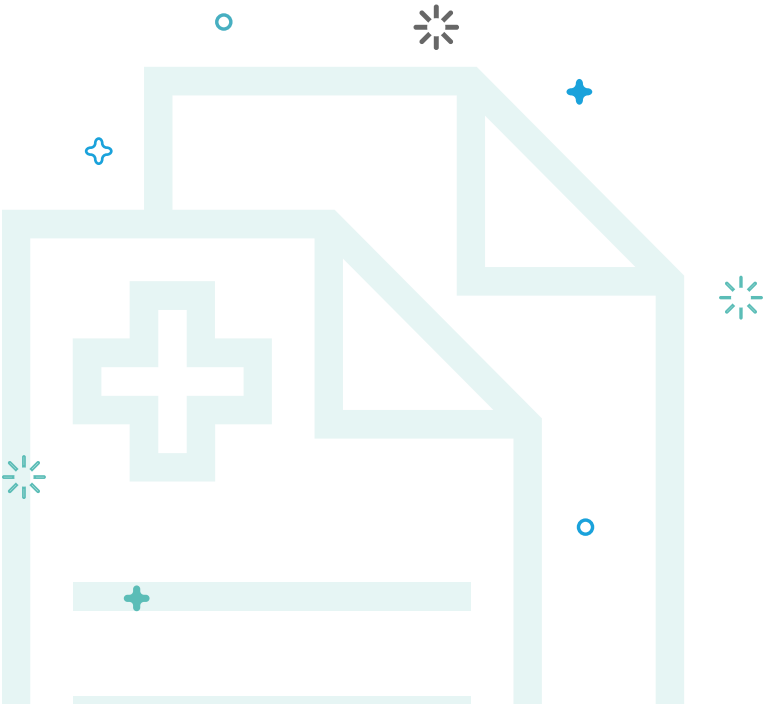
Afin d'intégrer les exigences de sécurité des données personnelles, une solution est de définir et implémenter un S-SDLC (Secure System Development Lifecycle) cycle sécurisé de développement de système.

7. Principe d'information

Les personnes doivent être informées de leurs droits et consentir explicitement à la collecte et au traitement de leurs données personnelles. De plus, en cas de fuite de données, les personnes concernées ainsi que la CNIL doivent être prévenues dans un délai de 72 heures.

Exemple | **Informer**

Le patient doit être informé de ses droits lors de la collecte. De plus, en cas de fuite de données, la CNIL et les personnes concernées doivent être prevenues. Cela implique de pouvoir détecter ces fuites de données. Pour cela un système de génération et de traitement d'événements de sécurité doit être mis en place. Il peut prendre la forme d'un SIEM (security information and event management) géré et opéré dans un SOC (security operational center).



6 étapes pour vous mettre en conformité avec le RGPD

1. Désigner un pilote et les structures de gouvernance
2. Cartographier les traitements
3. Prioriser les actions
4. Gérer les risques
5. Organiser les processus internes
6. Documenter la conformité

Témoignage de notre expert RGPD

Même si une bonne partie des exigences en matière de sécurité des données médicales imposées par le RGPD sont déjà en vigueur dans les établissements médicaux du fait des précédentes législations, ce règlement représente tout de même un véritable bouleversement pour la plupart des organisations.

Un point essentiel est l'accountability, le fait de pouvoir démontrer en permanence la conformité. Ce point impose la mise en œuvre d'un système de management de la sécurité de l'information (tel que définit dans la norme ISO 27001) et un pilotage de la sécurité par les risques.

Au delà des contraintes imposées par ce système de management, cela constitue une véritable opportunité d'engager une démarche d'architecture d'entreprise et de SSI qui permettra à moyen terme une meilleure maîtrise du système d'information, une rationalisation des moyens et une diffusion des bonnes pratiques de sécurité à l'ensemble des utilisateurs.

Témoignage du docteur Philippe Saury

Notre cabinet a confié à Versusconsulting la réalisation d'un audit d'évaluation de la conformité avec le RGPD de notre cabinet de chirurgie esthétique. Cela a commencé par un questionnaire permettant de vérifier 160 points de conformité. Cet outil est très bien conçu car il est rapide et les termes utilisés sont facilement compréhensibles par les néophytes en informatique que nous sommes. L'auditeur maîtrisant parfaitement son sujet, il a su nous guider et illustrer les différents enjeux par des cas pratiques nous permettant de mieux les appréhender. Un point ne nous concernait pas car en médecine, il n'y a pas de droit à l'oubli.

Dans un deuxième temps, nous avons eu une restitution au cours de laquelle Versusconsulting nous a exposé les préconisations découlant de l'audit et la démarche en 6 étapes pour nous mettre en conformité. Nous avons alors réalisé qu'il serait nécessaire de nous faire accompagner pour la mise en œuvre d'un plan d'actions n'ayant pas les compétences pour le faire en interne.

N'ayant aucune notion des enjeux et conséquences du RGPD, nous avons apprécié leur démarche structurée, pédagogique et rapide. Le dossier d'audit qu'ils nous ont remis nous a permis d'avoir une vision très claire de nos pratiques, des éventuels risques et d'une hiérarchisation des actions à mettre en œuvre.

En effet, nous pouvons d'ores et déjà nous conformer aux principes de gouvernance et accountability en formalisant un document sur notre politique de traitement des données personnelles. Ensuite, après avoir changé de logiciel patient, nous attaquerons la mise en place de sauvegardes avec stockage externe, l'obtention des consentements et la gestion d'un registre des traitements. Deux points pourront facilement être résolus grâce à la plateforme automatisée de gestion des traitements et consentements proposée par Versusconsulting.

Même si notre mise en conformité va engendrer un investissement temps et financier, elle va avant tout nous permettre de mieux structurer notre cabinet et nos outils pour assurer la gestion des données personnelles de nos patients en toute sécurité.

Chirurgien Plasticien - Villa Isabey

VILLA ISABEY
Cabinet Médico-Chirurgical

versushealth

Nous contacter

20 rue Isabey - 54000 Nancy

contact@versusmind.eu

Tél.: +33 (0)3 83 27 22 03

www.versushealth.com

www.rgpd-2018.com

www.versusmind.eu