DESMARAIS
AVOCATS

communiqué de presse

La CNIL libéralise la e-santé, ou presque…

Paris, le 22 mai 2017 • **L'information est tombée vendredi 19 mai 2017 et elle va sûrement faire du bruit : la CNIL a annoncé sur son site internet[1] que les traitements de données, nécessaires à des activités de télémédecine, de dossier médical partagé et d'éducation thérapeutique ne relèvent plus du régime d'autorisation préalable ! Pour Mr Pierre Desmarais, la conséquence est : *« une simple déclaration suffit désormais pour la mise en œuvre d'un traitement de données, soit un gain de temps de l'ordre de 18 à 24 mois ! ».***

Des délais plus rapides mais des contreparties fortes !

Cet allègement, assez considérable, du régime des formalités préalables anticipe l'entrée en vigueur du Règlement Général relatif à la Protection des Données (RGPD).

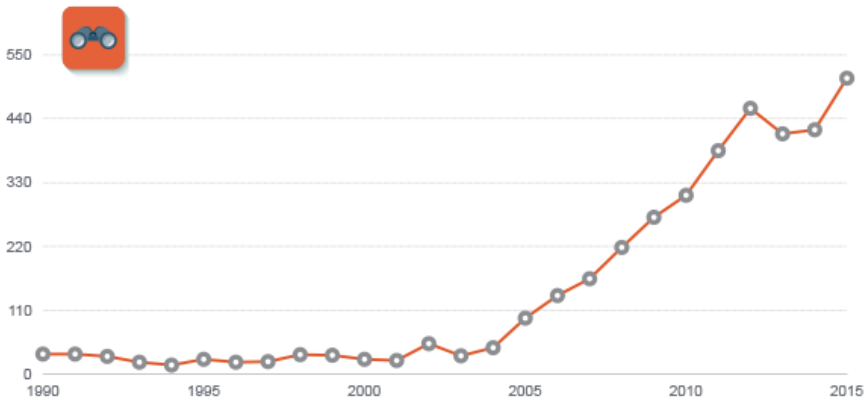
En contrepartie, les acteurs doivent davantage se responsabiliser, ce qui implique plusieurs conséquences :

- L'obligation d'établir un dossier de conformité, permettant à tout moment de démontrer la conformité du traitement aux principes énoncés dans le RGPD et aux mesures de sécurité standard.
- L'augmentation colossale des sanctions : la sanction administrative – de 3 000 000,00 d'euros d'amende depuis l'automne 2016 – va passer à 20 000 000,00 euros d'amende.
- L'augmentation du nombre de contrôles, comme la Commission l'explique : *« la CNIL se montrera également particulièrement vigilante sur les conditions de mise en œuvre des traitements de données de santé, notamment afin que le recueil du consentement s'effectue dans le cadre de la délivrance d'une information de qualité. Elle renforcera également son contrôle en aval, afin de s'assurer du respect effectif de ses préconisations ».*

A cet égard, deux points sont dignes d'intérêt :

- La forte augmentation du nombre de contrôles, lors de la réforme de la CNIL en 2004 destinée à renforcer ses pouvoirs de sanction :

Évolution du nombre annuel de contrôles entre 1990 et 2015

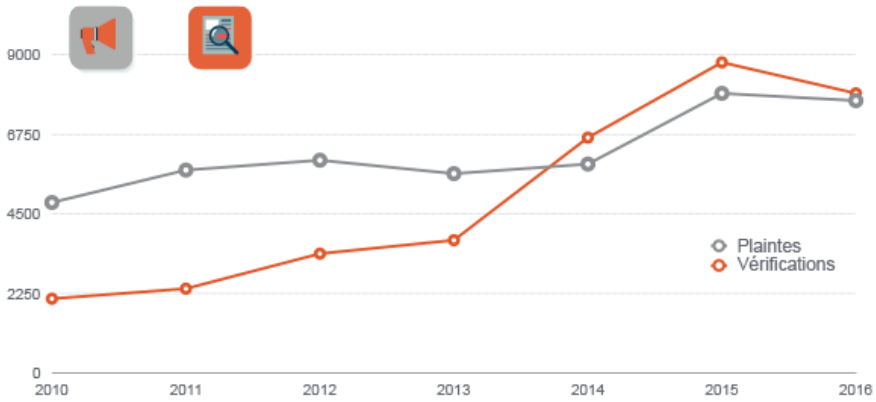


[1] https://www.cnil.fr/fr/traitement-des-donnees-de-sante-une-logique-de-simplification-et-de-responsabilisation-accrue-des

Contacts presse : **LauMa communication** • tel. 01 73 03 05 20
Manon Blanchard • tel. 01 73 03 05 26 • manon.blanchard@lauma-communication.com
Laurent Mignon • tel. 01 73 03 05 21 • laurent.mignon@lauma-communication.com

- L'explosion du nombre de plaintes déposées à la CNIL et de vérifications depuis 2015 :

Évolution du nombre annuel de plaintes et de vérifications de 2010 à 2016



Anticiper l'entrée en vigueur du RGDP

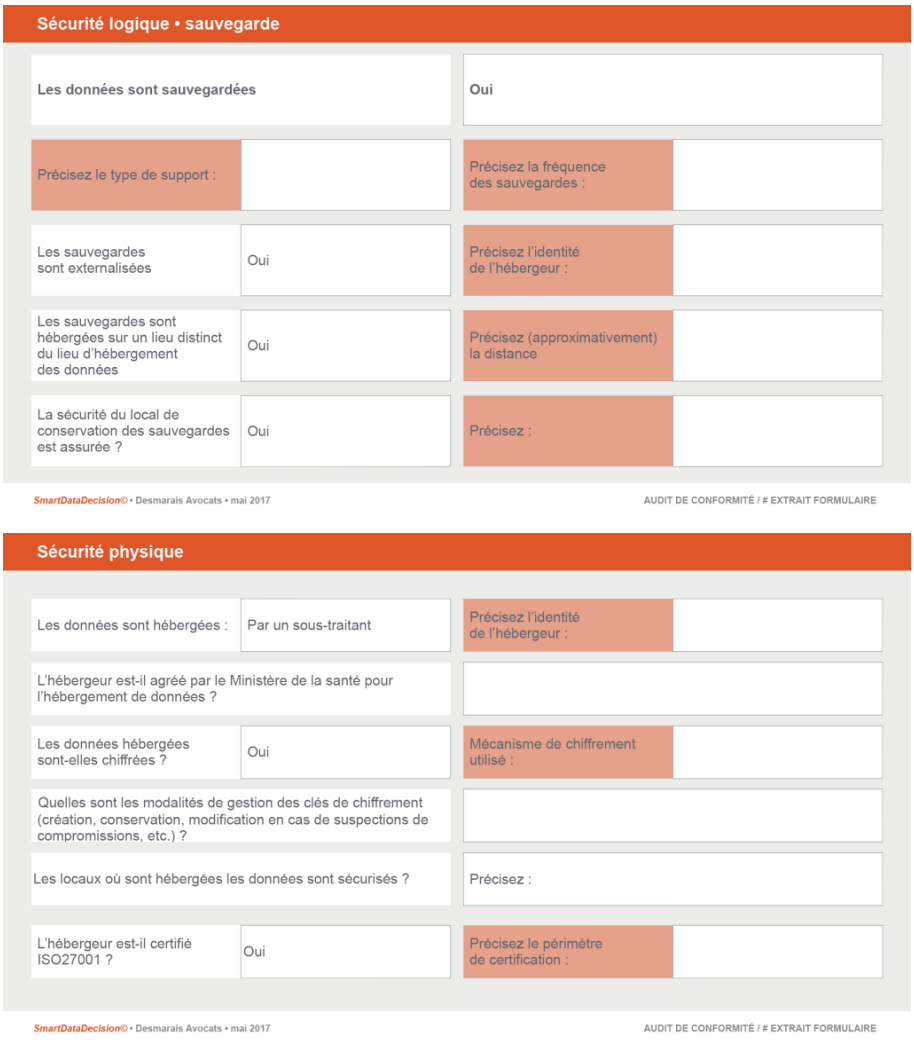
Afin d'accompagner chaque entreprise, Desmarais Avocat a élaboré une offre packagée permettant d'anticiper l'entrée en vigueur du RGPD en réalisant un audit de conformité.

L'offre "Anticipation du RGDP" comporte les éléments suivants :

- *Réunion de lancement (dans la limite de 4h) :* entretien avec les principaux « opérateurs » du traitement de données pour identifier :
  - Les caractéristiques du traitement.
  - Les sous-traitants.
  - Les transferts de données.
  - L'étude de la cartographie du SI.
- *Audit de conformité :*
  - Remise d'un formulaire « *Audit de Sécurité* » (pour évaluer l'écart et les impacts métier associés aux nécessités de mise en conformité) et aide à la complétion.
  - Etude des politiques de sécurité du système d'information, de mots de passe et de sauvegarde.
  - Analyse de la conformité.
  - Validation des caractéristiques des traitements (Désignation du responsable de traitement, formalités préalables applicables, durée de conservation, transferts hors UE, et audit de conformité).
  - Détermination des risques encourus en cas de non-conformité avec *SmartDataDecision*©.
- *Réunion d'aide à la définition des priorités (dans la limite de 3h) :* Préparation et animation d'une réunion pour définir le seuil d'acceptabilité du risque du responsable de traitement, les actions pertinentes et prioriser les actions en fonction du degré de risque.
- *Remise d'outils de pilotage des traitements de données :*
  - Outil de suivi des contrats de sous-traitance complété avec l'identité des sous-traitants.
  - Registre des traitements complété.
  - Matrice d'applicabilité des droits de la personne en fonction de la base juridique du traitement.
  - Clause type relative aux traitements de données par un sous-traitant.
  - Dossier de conformité du traitement de données.

Contacts presse : **LauMa communication** • tel. 01 73 03 05 20
Manon Blanchard • tel. 01 73 03 05 26 • manon.blanchard@lauma-communication.com
Laurent Mignon • tel. 01 73 03 05 21 • laurent.mignon@lauma-communication.com

La phase d'audit s'appuie sur un panel d'outils juridiques et métiers ayant déjà fait preuve de leur efficience. Il s'agit des missions précédentes de mise en conformité vis-à-vis du Règlement européen, et notamment sur *SmartDataDecision*©.



Sécurité logique • sauvegarde

Les données sont sauvegardées		Oui	
Précisez le type de support :		Précisez la fréquence des sauvegardes :	
Les sauvegardes sont externalisées	Oui	Précisez l'identité de l'hébergeur :	
Les sauvegardes sont hébergées sur un lieu distinct du lieu d'hébergement des données	Oui	Précisez (approximativement) la distance	
La sécurité du local de conservation des sauvegardes est assurée ?	Oui	Précisez :	

SmartDataDecision© • Desmarais Avocats • mai 2017 — AUDIT DE CONFORMITÉ / # EXTRAIT FORMULAIRE

Sécurité physique

Les données sont hébergées :	Par un sous-traitant	Précisez l'identité de l'hébergeur :	
L'hébergeur est-il agréé par le Ministère de la santé pour l'hébergement de données ?			
Les données hébergées sont-elles chiffrées ?	Oui	Mécanisme de chiffrement utilisé :	
Quelles sont les modalités de gestion des clés de chiffrement (création, conservation, modification en cas de suspections de compromissions, etc.) ?			
Les locaux où sont hébergées les données sont sécurisés ?		Précisez :	
L'hébergeur est-il certifié ISO27001 ?	Oui	Précisez le périmètre de certification :	

SmartDataDecision© • Desmarais Avocats • mai 2017 — AUDIT DE CONFORMITÉ / # EXTRAIT FORMULAIRE

SmartDataDecision© : les data analytics au service du juridique et réglementaire en e-santé

SmartDataDecision© est le 1er outil d'aide à la décision en matière de traitement de données, élaboré par Desmarais Avocats à partir de données *de vie réelle*. Alors que les responsables de traitement sont complètement perdus dans la jungle réglementaire et ont du mal à identifier les priorités, *SmartDataDecision*© permet de prendre rapidement des décisions relatives à un traitement de données en en mesurant les risques de façon visuelle.

Après la réalisation d'un audit, un tableau, simple à lire, avec des codes couleurs est remis au client. En zone verte, le risque est résiduel. En zone rouge, le risque est trop important, il faut agir. En zone orange, tout dépend du degré d'acceptabilité du risque par le client.

Avec *SmartDataDecision*©, la priorisation des mesures à engager et les décisions d'affectation des ressources – tant financières qu'humaines – sont non seulement facilitées, mais surtout faites en toute connaissance de cause.

Contacts presse : **LauMa communication** • tel. 01 73 03 05 20
Manon Blanchard • tel. 01 73 03 05 26 • manon.blanchard@lauma-communication.com
Laurent Mignon • tel. 01 73 03 05 21 • laurent.mignon@lauma-communication.com