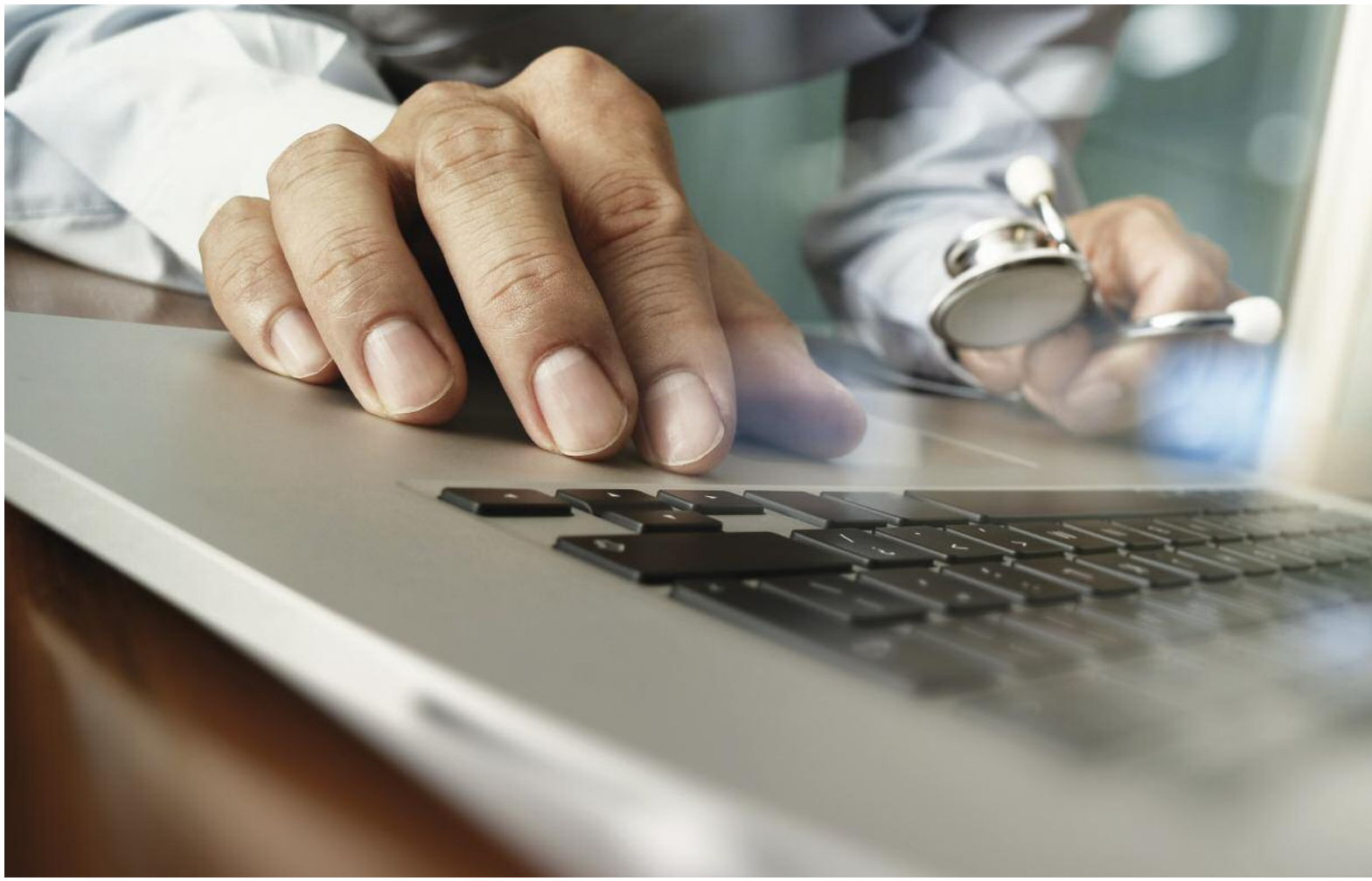


LES NOUVELLES OBLIGATIONS RÉGLEMENTAIRES EN MATIÈRE DE PROTECTION DES DONNÉES PERSONNELLES

MISE EN PLACE DU RGPD : CE QU'IL FAUT SAVOIR

Adopté le 27 avril 2016, le Règlement Général pour la Protection des Données (RGPD) entrera en vigueur le 25 mai 2018. Cette nouvelle réglementation européenne, qui vise à renforcer la protection des données personnelles, repose sur une plus grande responsabilisation des acteurs de traitements et de leurs sous-traitants. Si de nombreuses formalités auprès de la CNIL sont amenées à disparaître, les structures et entreprises concernées devront désormais assurer une protection appropriée des données dès la conception et par défaut, mais également être en mesure de démontrer leur conformité avec le règlement à tout moment. Des changements à anticiper dès maintenant, au regard des sanctions encourues.

PAR ANAÏS GUILBAUD

Avec la démocratisation des nouvelles technologies et en particulier l'émergence du Big Data, la protection de la vie privée représente un enjeu essentiel dont s'est emparée l'Union Européenne. La directive 95/46/CE, jusque-là règle en la matière, s'avérait en effet insuffisante au regard de l'évolution de la collecte et du traitement des données personnelles. Le Règlement Général pour la Protection des Données[1] promulgué en avril 2016, et dont l'entrée en application est prévue pour le 25 mai prochain, marque ainsi l'avènement d'un cadre juridique plus strict et unifié pour les États membres de l'Union. Comme l'explique Marguerite Brac de La Perrière, avocate et directrice du département santé numérique au sein du cabinet Lexing Alain Bensoussan Avocats : « *Il s'agit de créer un espace de confiance, permettant d'assurer aux personnes dont les données sont traitées le respect de leurs droits* ». Pour ce faire, le texte poursuit trois objectifs : renforcer les droits des personnes, notamment par la création d'un droit à la portabilité des données personnelles ; responsabiliser les acteurs traitant les données, qu'ils soient auteurs de traitement ou sous-traitants ; et enfin « crédibiliser la régulation » par la coopération renforcée entre les autorités de protection des données et des sanctions renforcées.

UNE PLUS GRANDE RESPONSABILISATION DES ACTEURS

Du côté des responsables de traitements, le RGPD s'inscrit donc dans une logique de responsabilisation et se caractérise par une inversion de la charge de la preuve. Alors que la directive de 1995 reposait en grande partie sur des formalités préalables de type déclaration auprès du régulateur, le nouveau règlement s'appuie quant à lui sur une logique de conformité. Si les démarches administratives s'en trouvent allégées – puisqu'il ne sera plus nécessaire de déclarer les traitements qui ne constituent pas un risque pour la vie privée des personnes - la responsabilité des acteurs de la chaîne de traitement des données sera en revanche renforcée. Chaque structure comptant plus de 250 employés, ou traitant des données sensibles, susceptibles de comporter un risque pour les droits et libertés des personnes concernées devra ainsi tenir un registre des traitements, dans lequel seront consignées notamment les mêmes informations que dans les déclarations préalables. La CNIL n'aura par ailleurs plus à démontrer les manquements d'un responsable de traitement puisque ce sera à ce dernier de prouver qu'il respecte le règlement. Autre nouveauté, cette responsabilité s'appliquera également aux sous-traitants.

Pour s'assurer la mise en œuvre de ces dispositions, l'institution européenne a assorti son texte de nouvelles sanctions. Comme l'explique Marguerite Brac de La Perrière : « *Jusque-là les sanctions encourues n'étaient pas réellement dissuasives, notamment au regard de l'investissement nécessaire à une mise en conformité* ». Cette époque est bel et bien révolue puisqu'à compter du 25 mai, les amendes pourront s'élever à 20 millions d'euros, ou dans le cas d'une entreprise jusqu'à 4% du chiffre d'affaires annuel mondial, le montant le plus élevé étant retenu. Un chiffre bien loin des 150 000 euros par infraction que la CNIL pouvait auparavant infliger. Et Marguerite Brac de La Perrière de poursuivre : « *Nous voyons déjà les effets de cette responsabilisation chez nos clients qui se bousculent pour cartographier leurs traitements, identifier les écarts à la réglementation, et entreprendre les actions nécessaires à leur mise en conformité. Si dans le domaine de la santé, les acteurs, respectueux du secret médical, étaient déjà sensibilités et relativement vigilants vis-à-vis de la protection des données, des adaptations organisationnelles, techniques et juridiques s'imposent, notamment face à l'évolution des outils numériques.* »

UNE PROTECTION PAR DÉFAUT ET DÈS LA CONCEPTION

En termes de sécurité des traitements, si concrètement le RGPD ne change pas vraiment la donne pour les professionnels du secteur médical et médico-social qui se référaient déjà aux référentiels sectoriels - en particulier à la Politique Générale de Sécurité des Systèmes d'Information de Santé (PGSSI-S) - sa philosophie repose tout de même sur de nouveaux fondements. En particulier, la protection des données devient obligatoire par défaut et dès la conception d'un produit ou service. Dorénavant, les responsables de traitement devront mettre en œuvre toutes les mesures techniques et organisationnelles nécessaires à une protection appropriée des données, et ce, dès leur collecte et jusqu'à leur suppression définitive. À ce titre, c'est une protection par défaut des moyens et conditions des traitements qui s'appliquera ainsi dès le 25 mai 2018.

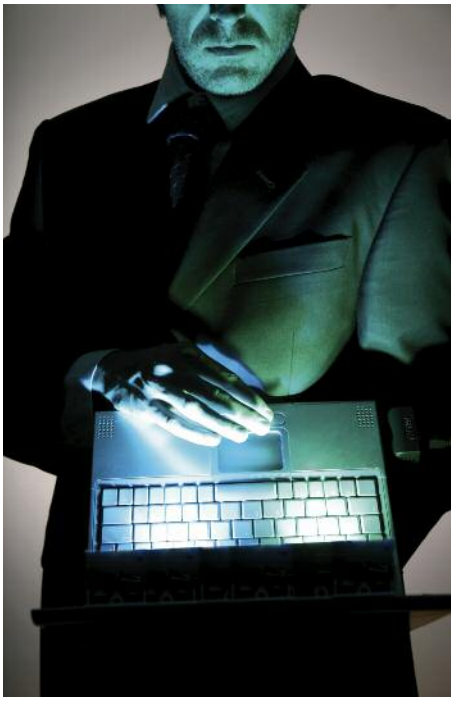
En parallèle, le texte introduit un principe dit « de minimisation ». Celui- ▶

▶ ci entérine le fait que le responsable du traitement devra être en capacité de garantir que « seules les données à caractère personnel qui sont nécessaires au regard de chaque finalité spécifique du traitement [seront] traitées » comme défini dans l'article 25 du règlement. Autrement dit, les responsables de traitement devront veiller dès le départ, à limiter la quantité de données traitées. De même, une fois la finalité du traitement atteinte, les données devront être systématiquement supprimées, sauf obligation de conservation légale particulière. Enfin, le RGDP introduit une obligation de notification en cas de violations de données. Les responsables de traitement devront ainsi notifier cette violation à la CNIL au plus tard dans les 72 heures après en avoir pris connaissance. L'information des personnes concernées sera quant à elle requise si cette violation est susceptible d'engendrer un risque élevé pour leurs droits et libertés.

LES OUTILS DE CONFORMITÉ

Afin de permettre à chaque entité une réelle mise en conformité avec son texte, l'Union Européenne a défini de nouveaux outils. Au-delà de la tenue d'un registre des traitements mis en œuvre et de la notification des failles de sécurité, la principale nouveauté repose sur la désignation d'un délégué à la protection des données[2], qui deviendra le garant de la conformité en matière de protection des données au sein de son organisme. Ses attributions lui donnent ainsi pour mission d'informer et de conseiller les personnels et sous-traitants sur les règles en la matière, de contrôler le respect du règlement, de conseiller son employeur sur la réalisation d'analyses d'impact, et enfin de faire le lien avec les autorités de contrôle. Ce poste deviendra obligatoire pour tous les établissements publics et entreprises qui effectuent des traitements sur des données sensibles ou des traitements à grande échelle. En revanche, rien n'empêche aux grandes entités, notamment aux GHT, de le mutualiser. Pour Marguerite Brac de La Perrière, dans l'idéal, le délégué à la protection des données devra se distinguer du Responsable de la Sécurité des Systèmes d'Information (RSSI) afin d'éviter d'éventuels conflits d'intérêts. Selon elle, il conviendrait de choisir quelqu'un « *qui a la possibilité de conduire ses missions en toute indépendance, d'obtenir les moyens de les réaliser, et qui rapporte au niveau le plus élevé de la direction* ».

Autre obligation pour les responsables de traitement à risques, la conduite d'une analyse de l'impact de ce dernier, précédant sa mise en œuvre. Cette analyse devra ainsi faire apparaître les caractéristiques du traitement, ses risques et les mesures adoptées pour les minimiser. En cas de risque élevé, il sera nécessaire de consulter l'autorité de protection des données, qui pourra ainsi s'opposer à sa mise en œuvre. Afin d'aider les responsables de traitement peu familiarisés avec cette démarche, la CNIL a développé un logiciel open source téléchargeable sur son site[3]. Enfin au regard des spécificités de chaque secteur, le RGPD encourage l'adhésion à des codes de conduite destinés à contribuer à sa bonne application. De même, la mise en place de mécanismes de certification ou de labels représente une possibilité supplémentaire pour s'assurer du respect du texte européen, comme c'est déjà le cas avec l'agrément hébergeurs de données de santé – bientôt transformé en certification.



COMMENT BIEN SE PRÉPARER ?

Comme le résume Marguerite Brac de La Perrière : « *Dans le monde de la santé, la sécurité des données passe par une stricte politique d'habilitations, des accès authentifiés à l'aide d'un moyen d'authentification forte, la traçabilité, le chiffrement des données ou des flux, et en tous cas des sauvegardes, et un hébergement sécurisé et dédié des données* ». Afin de guider les entreprises et organismes, la CNIL a d'ailleurs défini six étapes consultables sur son site[4]. Suite à la désignation d'un délégué à la protection des données, il convient donc d'entreprendre un travail de cartographie retraçant le cycle de vie complet d'une donnée. Les autres étapes mises en avant sont : la priorisation des actions à mener ; la réalisation d'analyses d'impact pour les traitements à risques ; la mise en place de procédures internes garantissant la prise en compte de la protection des données à tout moment ; et enfin la constitution d'une documentation permettant de prouver sa conformité avec le nouveau règlement. « *Il s'agit d'un travail d'envergure que de déterminer les écarts avec la réglementation*, met en garde Marguerite Brac de La Perrière. *Dans le cas d'un établissement de santé, il faudra analyser le cheminement des données de leur collecte à leur suppression définitive, c'est-à-dire processus par processus, et ce, service par service. Il y a donc lieu de se faire aider, sur les plans juridique et technique, afin d'être en mesure d'établir une feuille de route permettant d'arriver à une complète conformité*.»

1 - Pour consulter le règlement : https://www.cnil.fr/fr/reglement-europeen-protection-donnees
2 - Le délégué à la protection des données est souvent désigné par l'acronyme DPO pour Data Protection Officer.
3 - Le logiciel PIA est téléchargeable à l'adresse suivante : https://www.cnil.fr/fr/outil-pia-telechargez-et-installez-le-logiciel-de-la-cnil
4 - https://www.cnil.fr/fr/principes-cles/reglement-europeen-se-preparer-en-6-etapes