GUIDE

UTILISATEUR

INFOS PRATIQUES
Pour tout savoir sur le RGPD

Le Règlement Général sur la Protection des Données s'applique depuis le 25 mai 2018.

Il est temps de s'y conformer !
Ce guide vous explique comment faire.

SITE DE CAEN (Siège social)
Bâtiment COMETE 7 longue vue des astronomes 14111 Louvigny
02 50 53 70 00

SITE DE ROUEN
1231 rue de la sente aux bœufs 76160 Saint Martin du Vivier
02 32 80 91 50

contact@normand-esante.fr

Avant-propos

Le nouveau règlement européen (UE) 2016/79, relatif à la protection des données (RGPD) est applicable depuis le 25 mai 2018.

Le RGPD vise à renforcer l'importance de la protection des données personnelles auprès de ceux qui les traitent et à responsabiliser les professionnels. Le RGPD accroît les droits des citoyens en leur donnant plus de maîtrise sur leurs données.

En pratique, les formalités préalables actuelles auprès de la Commission Nationale de l'Informatique et Libertés (CNIL) ont disparu au profit d'une logique de conformité continue. Les organismes qui traitent des données personnelles devront veiller au respect des textes tout au long du cycle de vie de la donnée. En contrepartie de cette réduction du contrôle en amont, le RGPD renforce les pouvoirs de sanction de la CNIL.

Rôle du guide pratique

Ce guide pratique tente d'apporter des réponses concrètes et permettra de jouer un rôle essentiel en matière de protection des données et de la vie privée.

Il est destiné à l'ensemble des adhérents du GCS Normand'e-Santé (NeS), représentant divers acteurs du monde de la santé et à toute personne intéressée par la question des données personnelles dans le domaine de la santé. Il est mis à disposition sur le site internet de NeS.

Ce guide a donc été conçu afin de répondre le plus précisément possible aux différents acteurs de la santé. Il peut servir de première approche afin de se familiariser avec le RGPD et d'aide dans la mise en place d'un processus de mise en conformité.

Vous retrouverez en annexe tous les liens utiles nécessaires à votre mise en conformité et notamment les nombreuses informations du site internet de la CNIL.

Ce guide est divisé en 3 parties.

La 1ère partie présente de manière générale les règles importantes du RGPD que tous les acteurs de la santé devront respecter.

La 2ème partie explique les premières mesures à prendre en interne afin d'entamer une mise en conformité au RGPD.

Enfin, la 3ème partie de ce guide se décline en plusieurs fiches thématiques. Vous retrouverez ainsi une fiche complète sur le DPO (Data Protection Officer) afin de savoir si vous devez en nommer un et quelles missions lui seront attribuées, une fiche sur les premières mesures de sécurité à mettre en place en interne, une fiche concernant la gestion des données RH afin de sensibiliser la gestion du personnel dans les établissements concernés et enfin une fiche relative à la gestion d'un site internet lorsque votre établissement en possède un.

Bonne lecture !

Sommaire

Partie 1 : Présentation globale du RGPD

1 Le RGP quoi ?

Le RGPD est une règlementation européenne obligatoire qui refond et renforce les droits et la protection des données à caractère personnel des personnes physiques.

Le RGPD s'applique à toutes les structures quelle que soit leur taille, du moment que des données personnelles sont collectées.

Personne ne peut faire l'impasse sur le RGPD, tous les organismes intervenant dans le secteur de la santé doivent s'y conformer, y compris le médecin libéral qui exerce seul dans son cabinet.

Souvent perçu comme une lourdeur administrative en plus, le RGPD est surtout l'occasion de faire un point sur le traitement des données personnelles que chacun fait, et surtout de s'interroger et de mettre en œuvre les pratiques essentielles à la protection de celles-ci.

1.1 La protection des données personnelles, un enjeu particulièrement sensible

En tant que professionnel du secteur de la santé, vous êtes amenés à traiter des données qui relèvent de la vie privée des patients, et qui sont donc par nature très sensibles.

Leur divulgation peut porter atteinte aux droits et libertés des personnes concernées. C'est pourquoi ces données doivent être protégées de manière particulière.

Le respect du secret médical, tel que défini par l'article 1110-4 du Code de la Santé Publique (CSP) doit vous conduire à être particulièrement vigilant à l'égard de la protection des données à caractère personnel des patients, et par conséquent, à vous conformer aux obligations légales et règlementaires applicables en la matière.

La nouvelle règlementation doit être l'occasion pour chacun de revoir ses pratiques en matière de protection des données personnelles et d'adopter le bon comportement.

A cette occasion, il est notamment conseillé de vérifier que :

- La finalité de chacun des traitements et les éventuelles transmissions d'informations sont clairement définies
- Les dispositifs de sécurité informatiques et physiques sont précisément déterminés
- Les mesures d'information des personnes concernées sont appliquées.

1.2 Concrètement, avec le RGPD, on parle de quoi ?

1.2.1 Un traitement de données personnelles

Le RGPD vise à protéger les données personnelles.

Dès lors, qu'est-ce qu'une donnée à caractère personnel ?

Une donnée personnelle est « toute information se rapportant à une personne physique identifiée ou identifiable ».

Une personne physique peut donc être identifiée :

- Directement (nom ; prénom)
- Indirectement (par un identifiant, le numéro de sécurité sociale par exemple, un numéro de téléphone…)

Le RGPD donne pour la première fois une définition **des données de santé**. Les données de santé sont définies largement comme les 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.

Cette notion est très large. Et le RGPD s'applique dès lors qu'il y a un traitement sur ces données.

Cette notion de traitement est elle-même définie de manière large. En effet, un traitement de données personnelles est « une opération, ou ensemble d'opérations, portant sur des données personnelles, quel que soit le procédé utilisé (collecte, enregistrement, organisation, conservation, adaptation, modification, extraction, consultation, utilisation, communication).

1.2.2 Les acteurs

En premier lieu on retrouve le responsable de traitement. C'est la personne (physique ou morale) qui détermine les finalités et les moyens du traitement.

A côté du responsable de traitement, il est possible qu'un sous-traitant intervienne dans le traitement de données à caractère personnel (par exemple, il peut s'agir de l'hébergeur des données). Le sous-traitant est la personne qui agit pour le compte du responsable de traitement.

Enfin, le RGPD institue un nouveau rôle, celui de Délégué à la Protection des Données (DPD), plus couramment appelé DPO (pour Data Protection Officer).

D'emblée, il est nécessaire de préciser que la nomination d'un DPO, bien que recommandée, n'est pas obligatoire dans tous les cas.
Le RGPD prévoit 3 cas obligatoires dans lesquels un DPO doit être désigné :

- Lorsqu'il s'agit d'une autorité ou **d'un organisme public**
- Lorsque les activités de base du responsable de traitement consistent en un **traitement à grande échelle de données sensibles** (données de santé par exemple)
- Lorsque les activités de base du responsable de traitement consistent en un suivi régulier et systématique à grande échelle des personnes concernées

En dehors de ces cas, la nomination d'un DPO n'est pas obligatoire. En pratique, la question peut se poser de savoir ce qu'est un traitement de donnée à grande échelle. Il s'agit de prendre en compte la volumétrie des données, le nombre de personnes concernées…

Par souci de clarté, la CNIL a précisé que des médecins exerçant seuls ne sont pas soumis à l'obligation de nommer un DPO.
En revanche, lorsque des médecins exercent au sein d'un groupement, d'un centre hospitalier, il est convenu que ce groupement doive désigner un DPO.

2 Les principes clés

2.1 Les principes relatifs au traitement

Les données que vous collectez sur les patients doivent être adéquates, pertinentes et limitées à ce qui est strictement nécessaire à leur prise en charge au titre des activités de prévention, de diagnostic et de soins.

Exemple :
La collecte d'informations sur la vie familiale d'un patient n'est en principe pas appropriée.

Les données à caractère personnel ne peuvent être recueillies et traitées que pour une finalité déterminée, explicite et légitime, correspondant aux objectifs poursuivis par le responsable de traitement.

La finalité doit être respectée, il est impossible d'utiliser votre fichier pour un autre objectif que celui qui a été défini.

Conseil : Posez-vous les bonnes questions :

- Quel est le but de mon fichier ? (À quoi va-t-il servir ?)
- Est-ce légitime, notamment au regard de mes missions et des droits et libertés des personnes ?
- Comment présenter cette finalité pour la rendre compréhensible par tous (cf droit à l'information)

Attention !!
Tout détournement de finalité est passible de 5 ans d'emprisonnement et de 300 000 euros d'amende (article 226-21 du code pénal).

2.2 Le principe de licéité

Le RGPD interdit par principe les traitements de données de santé, sauf si une des exceptions est remplie (consentement, intérêt légitime…).

La CNIL s'est prononcée et à préciser que les professionnels de santé n'avaient pas besoin de recueillir le consentement des patients pour collecter et conserver les données de santé les concernant, dans la mesure où leur collecte et leur conservation sont nécessaires aux diagnostics médicaux et à la prise en charge sanitaire ou sociale des patients concernés.

Le consentement du patient ne sera pas nécessaire pour le partage et l'échange de données à des professionnels identifiés participant à la prise en charge du patient ou membres de l'équipe de soins. En dehors de ces cas, il faudra recueillir le consentement du patient (sauf si cela est nécessaire à la sauvegarde de l'intérêt vital de la personne).

Attention !!
Le consentement pour le traitement de données ne doit pas être confondu avec le consentement requis pour la réalisation de certains actes médicaux.
Par exemple, le consentement du patient sera toujours requis pour la réalisation d'un acte de télémédecine.

2.3 L'information aux personnes concernées

Le responsable de traitement doit prendre les mesures appropriées pour informer les personnes concernées.

Les informations à délivrer sont nombreuses (article 13 RGPD), en voici les principales :

- Les **coordonnées du responsable du traitement**
- Les coordonnées du délégué à la protection des données lorsqu'il y en a un
- **Les finalités** du traitement auxquelles sont destinées les données à caractère personnel
- Les intérêts légitimes poursuivis par le responsable du traitement ou par un tiers lorsque ces intérêts légitimes sont la condition de licéité du traitement
- Le fait que le responsable de traitement a l'intention d'effectuer un transfert de données à caractère personnel vers un pays tiers
- Le cas échéant, l'existence ou l'absence d'une décision d'adéquation rendue par la CNIL, la référence aux garanties appropriées ou adaptées et les moyens d'en obtenir une copie ou l'endroit où elles ont été mise à disposition
- **La durée de conservation** des données à caractère personnel ou, lorsque ce n'est pas possible, les critères utilisés pour déterminer cette durée
- **Les droits des personnes concernées :** l'accès aux données à caractère personnel, la rectification ou l'effacement de celles-ci, ou une limitation du traitement relatif à la personne concernée, ou du droit de s'opposer au traitement et du droit à la portabilité des données
- Lorsque le traitement est fondé sur le consentement de la personne concernée, **l'existence du droit de retirer son consentement** à tout moment, sans porter atteinte à la licéité du traitement fondé sur le consentement effectué avant le retrait de celui-ci
- Le droit d'introduire une réclamation auprès d'une autorité de contrôle

L'information doit être délivrée de façon concise, transparente, compréhensible et aisément accessible. Elle doit pouvoir être abordable par le grand public.

Bon à savoir :
Le support d'information est libre. Il est donc possible de donner l'information par écrit ou par un simple affichage dans une salle d'attente par exemple.

Lorsque l'acte réalisé requiert le consentement du patient (acte de télémédecine), cette information peut être donnée directement sur la note de consentement.

2.4 Le respect du droit des personnes

Les personnes concernées disposent de droits afin de garder la maitrise de leurs données.

Le responsable de traitement doit informer les personnes concernées de leurs droits et de la manière dont ils peuvent les exercer.

Le responsable de traitement doit donc s'assurer de l'effectivité des droits des personnes concernées.

Il doit être en mesure d'y répondre dans un délai de 1 mois, qui peut être prolongé de 2 mois supplémentaires compte tenu de la complexité et du nombre de demandes.

Les droits des personnes concernées sont les suivants :

- **Le droit d'accès** qui permet d'obtenir du responsable de traitement la confirmation que des données à caractère personnel la concernant sont ou ne sont pas traitées, et lorsqu'elles le sont d'en obtenir l'accès
- **Le droit de rectification** qui permet d'obtenir du responsable de traitement une modification des données lorsque celles-ci sont inexactes
- **Le droit à l'effacement** qui permet d'obtenir du responsable de traitement, dans les meilleurs délais, l'effacement des données à caractère personnel les concernant
- **Le droit à la portabilité** des données permet aux personnes concernées d'exiger des responsables de traitement la transmission de leurs données à caractère personnel à un autre responsable de traitement, sans que le responsable de traitement ayant initialement collecté les données puisse s'y opposer
- **Le droit à la limitation du traitement**
- **Le droit d'opposition** qui permet de s'opposer à tout moment à un traitement de données à caractère personnel

2.5 Le principe d'une durée de conservation limitée des données

Les informations figurant dans un fichier ne peuvent être conservées indéfiniment. Une durée de conservation doit être établie en fonction de la finalité de chaque fichier.

Toutefois, le CSP prévoit des durées minimales de conservation à respecter compte tenu du type de traitement qui est effectué. Définir une durée de conservation limitée dans le temps ne doit donc pas aller à l'encontre des durées de conservation prévues dans le CSP.

A titre d'exemple, les informations concernant la santé des patients constituées au sein des établissements de santé sont soient conservées au sein de cet établissement, soit hébergées pendant une durée de 20 ans ; à compter de la date du dernier séjour de son titulaire dans l'établissement ou de la dernière consultation externe en son sein.

2.6 L'analyse d'impact

La fin des formalités préalables est une innovation majeure du RGPD. Au préalable, avant de mettre en œuvre un traitement de données, vous deviez en informer la CNIL, et souvent prendre un engagement de conformité à une Norme Simplifiée (NS), une Autorisation Unique (AU), ou encore à un acte Règlementaire Unique (RU).

Dorénavant, il n'y a plus besoin de réaliser d'engagement de conformité à ces normes de référence (exception pour les méthodologies de référence lors d'un traitement ayant pour finalité des recherches dans le domaine de la santé).

En lieu et place des formalités préalables, il pourra être nécessaire de réaliser une étude d'impact sur la vie privée.

Cette étude consistera en une évaluation juridique et technique du traitement mis en œuvre sur les droits et libertés des personnes concernées.

Quand réaliser une analyse d'impact ?

Une analyse d'impact est obligatoire pour les traitements présentant un risque élevé pour les droits et libertés des personnes concernées. A partir du moment où des données de santé seront traités, il sera nécessaire de procéder à une analyse d'impact.

La CNIL a mis en place une dispense d'obligation de réaliser une analyse d'impact pour les traitements en cours régulièrement mis en œuvre (déclaration à la CNIL). Vous disposez d'un délai de 3 ans afin de réaliser une analyse d'impact.

En revanche, si votre traitement n'a pas été régulièrement mis en œuvre, vous devez réaliser au plus vite cette analyse d'impact.

Nb : Les anciennes normes de référence sont toujours disponibles sur le site de la CNIL et peuvent servir de support afin d'aider à la réalisation de l'analyse d'impact.

2.7 La tenue d'un registre des activités de traitement

Dès lors que vous traitez des données personnelles de manière habituelle, vous devez mettre en place un registre des activités de traitement.

Il s'agit d'un document de recensement et d'analyse qui doit refléter la réalité de vos traitements de données personnelles.

Dans ce registre, vous devez indiquer les parties prenantes (sous-traitant, co-responsables), les catégories de données traitées, la finalité du traitement, la durée de conservation, les modalités de sécurisation des données…

Comment réaliser ce registre ?

La CNIL a précisé que ce registre peut être mis en place dans un fichier Excel et a mis à disposition un modèle de registre.

Afin de faciliter la tenue de ce registre, NeS utilise un logiciel, le Data Privacy Manager, développé par son partenaire et qui est mis à disposition des membres de NeS (tarifs négociés).

2.8 Les principes de sécurité et de confidentialité

Vous devez respecter les règles de sécurité pour protéger les données des patients contre des accès non autorisés ou illicites et contre la perte, la destruction ou les dégâts d'origine accidentelle. Pour ce faire, vous devez mettre en place des mesures techniques et organisationnelles appropriées pour préserver la confidentialité et l'intégrité des données *(utilisation de la carte professionnelle de santé CPS, politique de gestion des mots de passe…).*

Sur la transmission des données :
Vous devez limiter l'accès aux données de santé de vos patients : seules certaines personnes sont autorisées, au regard de leurs missions, à accéder à celles-ci. Il s'agit des membres de l'équipe de soins du patient. Ces personnes n'accèdent qu'aux données nécessaires à l'exercice de leur mission.

Nb : Si vous souhaitez échanger des données avec des personnes non membres de l'équipe de soins, vous devez recueillir le consentement du patient. Dans ce cas, le consentement doit être clair et explicite sur les traitements de données qui seront faits. Vous devez garder une trace écrite de ce consentement.

2.9 Notifier une violation de données

Le RGPD impose aux responsables de traitement de documenter, en interne, les violations de données personnelles (nature de la violation, catégorie et nombre de personnes concernées, conséquences probables…) et de notifier les violations présentant un risque pour les droits et libertés des personnes à la CNIL, et dans certains cas, lorsque le risque est élevé, aux personnes concernées.

Une violation peut consister en **la perte de disponibilité, d'intégrité ou de confidentialité de données personnelles**, de manière accidentelle ou illicite.

Si vous devez notifier la violation à la CNIL (risque élevé pour les droits et libertés des personnes) vous devez notifier à la CNIL dans les 72 heures de la constatation de la violation.

2.10 Les sanctions

En cas de méconnaissance du RGPD, les responsables de traitement (y compris les organismes publics) peuvent faire l'objet de sanctions administratives importantes.

Les amendes administratives peuvent s'élever de 10 à 20 millions d'euros, ou dans le cas d'une entreprise, de 2% à 4% du chiffre d'affaire annuel mondial.

La CNIL peut également prononcer un avertissement, adresser une mise en demeure, limiter temporairement ou définitivement un traitement, ordonner de satisfaire aux droits des personnes…

Partie 2 : Méthodologie

Le RGPD est entré en application le 25 mai 2018. Depuis cette date, tous les responsables de traitement doivent être en conformité.

Consciente de la difficulté que cela représente pour certaines structures, la CNIL a communiqué afin de rassurer les nombreux acteurs, en affirmant que le 25 mai 2018 n'était pas une date « couperet ».

Cependant, même si vous n'êtes pas prêt depuis le 25 mai 2018, il est important d'initier, à l'aide de ce guide, une mise en conformité de votre structure au RGPD.

De nombreux guides sont parus, sur le site de la CNIL notamment (guide pour se mettre en conformité en 6 étapes, guide pratique pour les TPE-PME…). Il peut être utile de consulter ces guides afin de comprendre la mise en conformité. Une petite structure pourra par exemple trouver des réponses à ses questions avec le guide TPE-PME.

Le propos ici n'est donc pas de répéter l'ensemble de ces guides déjà mis en ligne mais de vous exposer, de manière la plus concrète possible, les actions à rapidement mener afin de mettre en place un processus de mise en conformité au RGPD.

3 Nommer une personne chargée de la protection des données

La mise en conformité au RGPD peut être complexe et nécessite une approche transversale de l'ensemble de l'activité d'une structure.

Un médecin libéral exerçant seul devra lui-même s'interroger sur les actions à mener afin notamment de protéger les données personnelles qu'il collecte. En revanche, une structure, avec plus de personnel, plus de données collectées doit assigner du temps à une personne qui se chargera d'avoir une vue d'ensemble afin d'entamer une mise en conformité au RGPD.

A retenir : afin d'assurer une mise en conformité efficace au RGPD, il est impossible que chaque service d'une même structure travaille séparément à la mise en conformité, d'où la nécessité de dégager du temps à une personne qui sera dédiée à cette mission.

Enfin, lorsque la structure se trouve dans l'obligation de désigner un DPO, il est évident que c'est celui-ci qui se chargera de cette mission.

Afin de savoir si vous devez désigner un DPO et l'étendue exacte de ses missions, reportez-vous à notre fiche thématique sur le DPO.

Nb : Même si vous n'êtes pas dans l'obligation de désigner un DPO, sachez que cette nomination est dans tous les cas fortement recommandée par la CNIL.

Dans tous les cas, la personne responsable de la mise en conformité sera chargée de réaliser les tâches suivantes.

4 Cartographier les données

Le RGPD est l'opportunité pour chacun de s'interroger sur les données collectées, leur utilisation et surtout les modalités mises en œuvre afin de les sécuriser.

A cette fin, la personne en charge des questions sur la protection des données devra dans un 1er temps réaliser l'inventaire de l'ensemble des données qui sont collectées (données RH, données patients, caméra de vidéo-surveillance…).

Cette étape permettra de faire une vraie mise au point, de recenser les déclarations qui avaient été préalablement faites à la CNIL.

Le résultat de cet inventaire apparaitra dans **le registre des traitements.** Ce registre est une nouvelle obligation qui s'impose à tous les responsables de traitement.

Chaque traitement doit être renseigné dans le registre, et doit contenir certaines informations.

Afin de vous aider à construire ce registre des activités de traitement, NeS propose une solution clé en main. Reportez-vous à la fiche thématique relative au registre des traitements afin d'avoir plus d'informations.

Nb : Lors de l'établissement de ce registre, n'oubliez pas le principe de minimisation des données. Si vous identifiez des données inutiles, n'hésitez pas à les supprimer définitivement.

5 Sécuriser les données

Garantissez l'intégrité de votre patrimoine de données en minimisant les risques de pertes de données ou de piratage.

Et plus les données traitées sont des données sensibles (données de santé des patients), plus il est nécessaire de prendre des mesures adéquates afin de les sécuriser.

Dans le cadre d'une mise en conformité, il y a différentes actions qui peuvent être mises en place afin de sécuriser les données.

Il peut s'agir par exemple de la mise à jour des logiciels et antivirus, d'une politique de sécurisation des mots de passe, des mesures de chiffrement des données, la mise en place d'une charte informatique et libertés à faire signer par l'ensemble du personnel, un accès aux locaux sécurisés…

Exemple sur la politique de gestion des mots de passe :

Oubliez tout de suite les post-it sur les ordinateurs ou les mots de passe « 0000 », « admin admin » ou « password ».

Privilégiez plutôt les mots de passe longs (12 caractères) avec différents caractères (majuscule, minuscule, chiffre, caractère spécial).

Et évidemment changez vos mots de passe régulièrement. Vos mots de passe ne doivent pas être toujours les mêmes. Construisez-vous des astuces mnémotechniques afin de les retenir (par exemple, les premières lettres d'une phrase…).

6 Le respect du droit des personnes

Le RGPD renforce le droit des personnes concernant leurs données personnelles. Vous devez vous assurer que vous êtes en mesure d'assurer ces droits.

Pour cela, il est impératif d'informer les personnes concernées sur leurs droits (voir les mentions d'information dans les principes généraux).

Il est donc indispensable en interne de prévoir le moyen pour que les personnes concernées exercent leur droit. Cela peut notamment se traduire par la communication des coordonnées de la personne en charge des données personnelles qui se chargera de faire droit à la demande de la personne concernée.

Attention !!
Vous disposez d'un délai d'1 mois afin de répondre à la demande de la personne concernée.
Toutefois, si la demande est complexe, ce délai peut être prolongé de 2 mois.

7 La documentation de la conformité

Attention !!
La mise en conformité au RGPD n'est pas le travail de quelques mois mais bel et bien un processus continu de responsabilisation vis-à-vis des données que vous collectez.

Il est donc nécessaire d'assurer un suivi concernant les questions relatives à la protection des données.

C'est pourquoi le registre des activités de traitement doit être un registre dynamique. Il doit être complété et mis à jour dès que cela est nécessaire.

Egalement, la personne en charge des questions relatives aux données personnelles doit conserver le consentement des personnes concernées lorsque celui-ci est recueilli ou encore le modèle des notes d'information qui sont transmises.

En résumé, la personne en charge des questions relatives à la protection des données recense l'ensemble des tâches effectuées concernant la protection et la sécurisation des données. Ce document permettra de prouver les actions menées pour la mise en conformité au RGPD.

Partie 3 : Les fiches thématiques

8 Le DPO

8.1 Obligation de désigner un DPO

La désignation d'un DPO est obligatoire dans les cas de figure suivants :

- Le traitement est effectué par une autorité ou un organisme public
- Les activités principales du responsable de traitement consistent à réaliser un suivi régulier et systématique des personnes à grande échelle
- Les activités principales du responsable de traitement à traiter à grande échelle des données sensibles telles que des données de santé

Il n'y a pas de définition précise d'un traitement de données à « grande échelle ». En revanche, il est recommandé de prendre en compte certains critères comme le nombre de personnes concernées, la sensibilité des données ou encore la volumétrie des données.

Ainsi, une distinction peut se faire selon les acteurs du domaine de la santé. Un médecin libéral n'aura pas l'obligation de nommer un DPO à l'inverse d'un hôpital par exemple.

S'il peut être facile de se prononcer sur l'obligation de désigner un DPO dans des exemples tels que des médecins libéraux exerçant seul ou des hôpitaux, cela peut s'avérer plus complexes dans certaines structures intervenant dans le monde de la santé.

En tout état de cause, le responsable de traitement devra motiver son choix et garder une trace de cette motivation. Si les traitements effectués par le responsable de traitement évoluent, il peut et doit revenir sur sa décision de nommer un DPO ou non.

Lorsqu'avec certitude on ne rentre pas dans l'un des trois critères de nomination, la désignation d'un DPO n'est pas obligatoire. Cependant, il est possible, et même recommandé de désigner un DPO.

Lorsqu'un DPO est désigné, le responsable de traitement est tenu de publier les informations relatives au délégué à la protection des données et de les communiquer à la CNIL.

Il est à noter que les responsables de traitement peuvent opter pour un DPO mutualisé ou externalisé.

8.2 Obligations et missions du DPO

Le RGPD impose des obligations importantes aux délégués à la protection des données. Le DPO est le pilote de la mise en conformité au RGPD au sein de son organisme.

Le DPO est notamment chargé de :

- Informer et conseiller le responsable de traitement ou le sous-traitant, ainsi que leurs employés
- S'assurer du respect de l'ensemble de la règlementation en matière de protection des données
- Conseiller l'organisme sur la réalisation d'études d'impact sur la protection des données et d'en vérifier l'exécution
- Coopérer avec l'autorité de contrôle (CNIL) et d'être le contact de celle-ci

Afin d'assurer la bonne mise en œuvre de ses missions, le DPO doit être en mesure, au sein de son organisme de :

- S'informer sur le contenu des nouvelles obligations
- Sensibiliser les décideurs sur l'impact de ces nouvelles règles
- Réaliser l'inventaire des traitements de données de votre organisme
- Concevoir des actions de sensibilisation
- Piloter la conformité en continu

En conséquence, la personne qui agit en tant que DPO endossera d'importantes responsabilités.

8.3 Le rôle de NeS

NeS se renforce pour se mettre en conformité pour ses propres traitements et envisage de proposer à ses adhérents un « service de DPO mutualisé ».

9 Les mesures de sécurité

9.1 Les mesures de sécurité physiques

Il est nécessaire de mettre en place des mesures de sécurité physique dans chaque lieu où il est possible d'accéder à des données à caractère personnel.

Il est notamment conseiller de :

- Limiter l'accès à l'établissement
- Ne pas stocker ou archiver des dossiers ou documents contenant des données à caractère personnel dans des bureaux accessibles à tous
- Installer des alarmes dans les locaux de l'établissement

9.2 Les mesures de sécurité numérique

La mise en œuvre des mesures de sécurité permet de garantir un niveau de sécurité adapté au risque.

Il est notamment conseillé de :

- Authentifier les utilisateurs : mettre en place un mot de passe de minimum 12 caractères contenant une majuscule, une minuscule, un chiffre et un caractère spécial ; ne pas le partager ; ne pas le noter en clair sur une feuille ; éviter de le préenregistrer ; le changer régulièrement
- Gérer les habilitations et sensibiliser les utilisateurs : déterminer les personnes qui sont habilitées à accéder aux données à caractère personnel ; supprimer les permissions d'accès obsolètes ; rédiger une charte informatique et l'annexer au règlement intérieur lorsqu'il en existe un
- Sécuriser l'informatique mobile : prévoir des moyens de chiffrement pour les ordinateurs portables et les unités de stockage amovibles (clés USB, CD…), éviter d'y stocker des données à caractère personnel sensibles des patients
- Sauvegarder et prévoir la continuité d'activité : mettre en place des sauvegardes régulières, stocker les supports de sauvegarde dans un endroit sûr…

10 Le traitement des données RH

Il a beaucoup été question dans ce guide des données de santé des patients, étant des données sensibles, elles demandent évidemment une vigilance accrue.

Cependant, il ne faut pas perdre de vue que le RGPD s'applique à l'ensemble des données personnelles.

Et dans la mesure où plusieurs personnes travaillent au sein de votre établissement, vous devez nécessairement traiter de la donnée RH, que ce soit pour la gestion administrative du personnel, la gestion de la paie ou encore le recrutement d'un collaborateur.

10.1 Quelles sont les données qu'un établissement peut collecter dans le cadre d'un traitement RH ?

10.1.1 Recrutement

Dans le cadre du recrutement, les données ne doivent servir qu'à évaluer la capacité du candidat à occuper l'emploi proposé.

Seules les données relatives à la qualification et à l'expérience du collaborateur peuvent être collectées (diplômes, emplois précédents…).

Il est donc interdit de :

- Demander à un candidat son numéro de sécurité sociale
- Collecter des données sur la famille du candidat
- Collecter des données sur les opinions politique ou l'appartenance syndicale du candidat

10.1.2 Gestion administrative du personnel

Dans le cadre de la gestion de ses collaborateurs et de manière plus générale, de son personnel, l'établissement employeur peut collecter principalement deux types de données :

- Des données nécessaires au respect d'une obligation légale
- Des données utiles à la gestion administrative du personnel, à l'organisation du travail et à l'action sociale

10.1.3 Contrôle de l'activité du personnel

L'établissement employeur peut mettre en place différents outils afin de contrôler l'activité des collaborateurs ou du personnel.

Par exemple, l'établissement pourrait encadrer les conditions d'utilisation d'internet par le personnel sur le lieu de travail. Il peut mettre en place des filtres afin de bloquer certains contenus. Il est également possible de limiter l'utilisation d'internet pour des raisons de sécurité par exemple le téléchargement de logiciels, la connexion à un forum…

Conseil : Elaborer une charte informatique.

Attention !!
Ne pas oublier que les principes relatifs au traitement de données s'appliquent également dans le cadre des données RH.
L'établissement ne peut collecter que des données adéquates, pertinentes et strictement nécessaires à la finalité du traitement.

Le responsable du traitement doit également définir une durée de conservation des données, inscrire le traitement au sein du registre…

Nb : Concernant le droit à l'information, l'employeur, responsable de traitement, est tenu des mêmes obligations mais rien ne s'oppose à ce que cette information soit directement délivrée dans le contrat de travail ou encore à ce qu'elle fasse l'objet d'un affichage ou d'une communication par courriel, notamment pour régulariser la situation auprès du personnel qui n'a pas été correctement informé.

11 Les sites internet

Les établissements peuvent créer des sites internet dans le cadre de leur activité professionnelle afin de promouvoir leurs activités, présenter les membres du personnel, exposer leurs compétences ou encore publier des articles.

Mais le site internet peut aussi permettre de collecter des données à caractère personnel par divers moyens :

- Un questionnaire en ligne
- Une consultation en ligne
- Un formulaire de contact
- La création d'un compte en ligne
- Des cookies…

11.1 Les mentions

Plusieurs informations doivent figurer sur le site internet de l'établissement :

- Les mentions légales
- Les mentions obligatoires du RGPD (information des personnes concernées)
- Les mentions d'informations relatives aux cookies

11.2 Qu'est-ce qu'un cookie ?

Les cookies sont des traceurs déposés et lus lors de la consultation du site internet de la structure, de la lecture d'un courrier électronique, de l'installation ou de l'utilisation d'un logiciel.

Les cookies et autres traceurs ont généralement pour finalité d'analyser la navigation et la fréquentation du site internet de la structure.

11.3 Comment rendre conforme l'utilisation des cookies licites ?

Dans un premier temps, il convient de vérifier la présence effective de cookies sur le site internet de la structure (par le biais du service informatique, des prestataires…).

Ensuite, il convient de déterminer les types de cookies utilisés sur le site internet de la structure.

En effet, certains cookies nécessitent le consentement de l'utilisateur :

- Les cookies publicitaires
- Les cookies « réseaux sociaux » générés par les boutons de partage lorsqu'ils collectent des données à caractère personnel sans consentement des personnes concernées
- Certains cookies de mesure d'audience

Dans ce cas, le consentement doit être préalable à l'insertion ou à la lecture de cookies. Tant que l'internaute n'a pas donné son consentement, ces cookies ne peuvent être déposés ou lus sur son terminal.

Liens utiles

https://www.cnil.fr/fr/reglement-europeen-protection-donnees

https://www.cnil.fr/fr/quest-ce-ce-quune-donnee-de-sante

https://www.cnil.fr/fr/rgpd-et-donnees-de-sante