TOUT SAVOIR

Le RGPD en Santé pour LES NULS

La sécurité numérique des données

RÈGLEMENT GÉNÉRAL SUR LA PROTECTION DES DONNÉES

GHT SOMME LITTORAL SUD

Ce document a été rédigé à partir des données légales du RGPD, et fortement argumenté et emprunté des analyses de la CNIL.
Il a pour but de vous informer sur les droits fondamentaux liés à la vie privée.
La page de garde est inspirée de la collection « Pour les nuls » de First Editions.

Dr. Yves JOUCHOUX – DPO CHU Amiens et GHT Somme Littoral Sud ;

jouchoux.yves@chu-amiens.fr

20 Aout 2018

LA LOI

Suite à l'adoption de la loi 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, dite « loi Informatique et libertés », la France a été l'un des premiers pays à créer une législation globale relative à la protection des données à caractère personnel. Cette loi a fait l'objet d'évolutions qui sont venues encadrer un certain nombre de traitements de données spécifiques.

La dernière modification provient de l'entrée en vigueur de la loi 2016-1321 du 7 octobre 2016 (loi pour une République numérique), venue renforcer certains pouvoirs accordés à la CNIL ainsi que les droits des personnes concernées.

Le droit européen en matière de protection des données personnelles est issu de la directive 95/46 du 24 octobre 1995 dont le but essentiel était d'harmoniser les législations des différents états de l'UE.

Cette directive a été transposée en droit français par la loi 2004-801 du 6 août 2004. Toutefois, cette loi insatisfaisante ne garantissait pas l'harmonisation des procédures et des sanctions entre les différents Etats européens.

Devant l'importance grandissante des problématiques liées aux données personnelles, le Parlement Européen a souhaité encadrer de manière plus stricte les législations des différents Etats, en adoptant le règlement 2016/679 du 27 avril 2016.

Ce règlement est dénommé « **Règlement Général sur la Protection des Données** » (RGPD) (« General Data Protection Regulation » ou GDPR), applicable depuis le 25 mai 2018 et transcrit en droit français par la **Loi n° 2018-493 du 20 juin 2018.**

Le RGPD est donc une évolution plus contraignante d'une réglementation issue de la loi « Informatique et Liberté » .

UNE DONNEE A CARACTERE PERSONNEL, C'EST QUOI ?

C'est toute information relative à une personne physique susceptible d'être identifiée, directement ou indirectement.

Par exemple : *un nom, une photo, une empreinte, une adresse postale, une adresse mail, un numéro de téléphone, un numéro de sécurité sociale, un matricule interne, une adresse IP, un identifiant de connexion informatique, un enregistrement vocal, ou un ou plusieurs éléments spécifiques propre à l'identité physique, physiologique, génétique, psychique, économique, social, géolocalisation etc.*

Peu importe que ces informations soient confidentielles ou publiques.

A noter *: pour que ces données ne soient plus considérées comme personnelles, elles doivent être* ***rendues anonymes*** *de manière à rendre impossible toute identification de la personne concernée : noms masqués, visages floutés, etc.*

Attention *: s'il est possible par recoupement de plusieurs informations (âge, sexe, ville, diplôme, etc.) ou par l'utilisation de moyens techniques divers, d'identifier une personne, les données sont toujours considérées comme personnelles.*

En santé : ***Nous collectons en permanence et massivement des données personnelles. Il nous faut les sécuriser, et réfléchir à la pertinence de leur collecte.***

UN TRAITEMENT DE DONNEES A CARACTERE PERSONNEL, C'EST QUOI ?

C'est toute opération portant sur des données personnelles, quel que soit le procédé utilisé.

Il s'agit de toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données à caractère personnel: la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction.

Par exemple : *enregistrer, organiser, conserver, modifier, rapprocher avec d'autres données, transmettre, etc… des données personnelles.*

Des fichiers mais pas seulement :

- Un traitement n'est donc pas uniquement un fichier, une base de données ou un tableau Excel. Il peut s'agir aussi d'une installation de vidéosurveillance, d'un système de paiement par carte bancaire ou de reconnaissance biométrique, d'une application pour smartphone, etc…
- Des traitements apparaissent et évoluent selon les innovations technologiques.

Informatisés mais pas uniquement :

- Un traitement de données à caractère personnel peut être informatisé ou non ;
- Un fichier papier organisé selon un plan de classement, des formulaires papiers nominatifs ou des dossiers de candidatures classés par ordre alphabétique ou chronologique sont aussi des traitements de données personnelles.

En santé : ***Nous devons être vigilants pour les travaux de recherche, de thèse, de publication, voire les fichiers intermédiaires conservés sur des supports variables et utilisés à des fins de gestion de service. Une grande vigilance doit être accordée aux disques externes et clefs USB.***

UNE DONNEE SENSIBLE, C'EST QUOI ?

C'est une information qui révèle les origines raciales ou ethniques, les opinions politiques, philosophiques ou religieuses, l'appartenance syndicale, la santé ou la vie sexuelle d'une personne physique, les données génétiques, biométriques.

Il est interdit de recueillir et d'utiliser ces données. Sauf dans certains cas précis et notamment :

- Si la personne concernée a donné son **consentement exprès** (écrit, clair et explicite) ;
- Si ces données sont nécessaires dans un **but médical** ou pour la recherche dans le domaine de la santé ;
- Si leur utilisation est justifiée par l'**intérêt public et autorisé par la CNIL** ;
- Si elles concernent les **membres ou adhérents d'une association** ou d'une organisation politique, religieuse, philosophique, politique ou syndicale.

A noter : Les informations relatives aux infractions ou condamnations ne sont pas considérées comme des données sensibles mais elles font l'objet de la même protection. Seules les juridictions et certaines autorités publiques peuvent les utiliser, ainsi que la personne morale victime dans le cadre de la défense de ses intérêts.

En santé : Il nous faut réfléchir à la pertinence des données collectées.

QUELS SONT LES GRANDS PRINCIPES DES REGLES DE PROTECTION DES DONNEES PERSONNELLES ?

Les **5 grands principes** des règles de protection des données personnelles sont les suivants :

1. **Finalité** : le responsable d'un fichier ne peut enregistrer et utiliser des informations sur des personnes physiques que dans un but bien précis, légal et légitime ;
2. **Proportionnalité et pertinence** : les informations enregistrées doivent être pertinentes et strictement nécessaires au regard de la finalité du fichier ;
3. **Durée de conservation limitée** : il n'est pas possible de conserver des informations sur des personnes physiques dans un fichier pour une durée indéfinie. Une durée de conservation précise doit être fixée, en fonction du type d'information enregistrée et de la finalité du fichier ;
4. **Sécurité et confidentialité** : le responsable du fichier doit garantir la sécurité et la confidentialité des informations qu'il détient. Il doit en particulier veiller à ce que seules les personnes autorisées aient accès à ces informations ;
5. **Droits des personnes.**

LA FINALITE D'UN FICHIER, C'EST QUOI ?

La finalité c'est le but poursuivi par le fichier créé : à quoi va-t-il servir ?

Exemples : *gestion du recrutement, gestion de la clientèle, enquête de satisfaction, protection des biens et des personnes, enquête scientifique etc.*

Lorsque vous déclarez un fichier à votre DPO ou à la CNIL, vous indiquez obligatoirement sa finalité : c'est cette finalité déclarée que vous aurez à respecter tout au long de la construction et de l'utilisation de votre fichier.

- La finalité doit être **déterminée**, **légitime et explicite** : il faut définir un but à votre fichier, ce but doit correspondre à votre activité professionnelle ou associative et il doit être clair et compréhensible ;
- La finalité doit être **respectée** : vous ne pouvez pas utiliser votre fichier pour un autre but que celui qui a été fixé. Ainsi, un fichier de recrutement ne peut pas être utilisé pour proposer des offres commerciales aux candidats à un emploi dans une société ;
- La finalité permet ensuite de déterminer **la pertinence des données personnelles** que vous recueillez. ***Par exemple,*** *il n'est pas pertinent de demander le numéro de sécurité sociale d'un client achetant un meuble dans un magasin ;*
- La finalité permet enfin de fixer la **durée de conservation des données** dans le fichier: en fonction du but poursuivi, les informations enregistrées dans le fichier devront être conservées plus ou moins longtemps. Par exemple, lorsqu'un adhérent quitte une association, ses données doivent être supprimées.

Attention : le détournement de finalité est une infraction pénale !

Les données à caractère personnel doivent être : […]

c) adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées (minimisation des données);
e) conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées; les données à caractère personnel peuvent être conservées pour des durées plus longues dans la mesure où elles seront traitées exclusivement à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques conformément à l'article 89, paragraphe 1, pour autant que soient mises en œuvre les mesures techniques et organisationnelles appropriées requises par le présent règlement afin de garantir les droits et libertés de la personne concernée (limitation de la conservation);
f) traitées de façon à garantir une sécurité appropriée des données à caractère personnel, y compris la protection contre le traitement non autorisé ou illicite et contre la perte, la destruction ou les dégâts d'origine accidentelle, à l'aide de mesures techniques ou organisationnelles appropriées (intégrité et confidentialité);
*(**Article 5 du Règlement général sur la protection des données**)*

QUELLE EST LA DUREE DE CONSERVATION DES DONNEES ?

La durée de conservation doit être définie par le responsable du fichier, sauf si un texte impose une durée précise. Cette durée va dépendre de la nature des données et des objectifs poursuivis.

Exemples de durées de conservation :

- Dans le cas d'un dispositif de **vidéosurveillance** poursuivant un objectif de sécurité des biens et des personnes, la conservation des images ne peut excéder 1 mois.
- Les données relatives à **gestion de la paie ou au contrôle des horaires des salariés** peuvent être conservées pendant 5 ans.
- Les données figurant dans un **dossier médical** doivent être conservées 10 ans à compter de la consolidation du dommage.
- La Cnil recommande que les coordonnées d'un prospect qui ne répond à aucune sollicitation pendant 3 ans soient supprimées.

Les données personnelles doivent donc être conservées et accessibles par les services opérationnels uniquement le temps nécessaire à l'accomplissement de l'objectif poursuivi lors de leur collecte.

***Par exemple**, lors d'un achat sur internet, les coordonnées de la carte bancaire du client ne peuvent être conservées que le temps de réalisation de l'opération de paiement*.

Ainsi, au terme de la réalisation de cet objectif, les données doivent être :

- effacées ou ;
- archivées ou ;
- faire l'objet d'un processus d'anonymisation des données, afin de rendre impossible la « ré-identification » des personnes. Ces données, n'étant plus des données à caractère personnel, peuvent ainsi être conservées librement et valorisées notamment par la production de statistiques.

En cas de procédure de suppression automatique, le responsable du fichier doit s'assurer que les données sont effectivement supprimées.

Le cycle de vie des données

Le cycle de conservation des données à caractère personnel peut être divisé en trois phases successives distinctes :

1. **1ère phase : La base active.**

C'est la durée d'utilisation courante des données ou autrement dit, la durée nécessaire à la réalisation de la finalité du traitement.

2. **2ème phase : L'archivage intermédiaire**

Il peut être justifié que les données personnelles soient conservées pour des durées plus longues en archivage intermédiaire distinctement de la base active, avec accès restreint, dans la mesure où :

- Il existe une obligation légale de conservation de données pendant une durée fixée ;
- En l'absence d'obligation de conservation, ces données présentent néanmoins un intérêt administratif, notamment en cas de contentieux, justifiant de les conserver le temps des règles de prescription/forclusion applicables, notamment en matière commerciale, civile et fiscale ;
- Enfin, sous réserve de garanties appropriées pour les droits et libertés des personnes concernées, certaines données peuvent être traitées exclusivement à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques.

Par exemple, une fois la transaction effectuée, les numéros de carte bancaire pourront être conservés en « archivage intermédiaire » en cas d'éventuelle contestation de la transaction pour une durée de 13 mois conformément.

3. 3ème phase : l'archivage définitif

Enfin, l'intérêt public peut parfois justifier que certaines données ne fassent l'objet d'aucune destruction : c'est l'archivage définitif. Ces archives sont gérées par les services des archives territorialement compétents.

Un archivage sélectif

Dans le cas d'un archivage intermédiaire, le responsable du fichier doit veiller à ne conserver que les données nécessaires au respect de l'obligation prévue ou lui permettant de faire valoir un droit en justice : un tri doit donc être effectué parmi la totalité des données collectées pour ne garder que les seules données indispensables.

Attention : *les données ainsi archivées ne peuvent pas continuer à être utilisées par les services opérationnels. Ces données ne sont désormais conservées que dans une optique contentieuse et ne sont accessibles que de façon restreinte*.

Un archivage limité dans le temps

Les données ainsi archivées ne sont conservées que le temps nécessaire à l'accomplissement de l'objectif poursuivi : elles doivent donc être supprimées lorsque le motif justifiant leur archivage n'a plus raison d'être.

Par exemple, *des données archivées pour se prémunir d'une action en justice durant le temps d'une prescription ou d'une forclusion doivent être supprimées lorsque cette action est prescrite forclose*.

Les modalités techniques d'archivage

Pour les archives intermédiaires, le choix du mode d'archivage est laissé à l'appréciation du responsable du fichier. Des données peuvent ainsi être archivées :

- dans une base d'archive spécifique, distincte de la base active, avec des accès restreints aux seules personnes ayant un intérêt à en connaitre en raison de leurs fonctions (par exemple, le service du contentieux) ;
- ou dans la base active, à condition de procéder à un isolement des données archivées au moyen d'une séparation logique (gestion des droits d'accès et des habilitations) pour les rendre inaccessibles aux personnes n'ayant plus d'intérêt à les traiter.

Pour les archives définitives (c'est- à-dire les données conservées dans l'intérêt public), il est recommandé de les conserver sur un support physique indépendant, non accessible par les systèmes de production, n'autorisant qu'un accès distinct, ponctuel et précisément motivé auprès d'un service spécifique seul habilité à les consulter (par exemple, la direction des archives lorsqu'elle existe).

Un archivage sécurisé

Des mesures techniques et organisationnelles doivent être prévues pour protéger les données archivées (destruction, perte, altération, diffusion ou accès non autorisés...). Ces mesures doivent assurer un niveau de sécurité approprié aux risques et à la nature des données.

Si des mesures de sécurité informatiques sont indispensables, n'oubliez pas de prévoir également des mesures de sécurité physique, notamment lorsque des dossiers sont archivés sous format papier.

Lorsque l'archivage est confié à un sous-traitant, le responsable du fichier doit s'assurer que son prestataire présente des garanties suffisantes en matière de sécurité et la confidentialité des données qui lui sont confiées.

Quel que soit le type d'archive, la consultation des données archivées doit être tracée.

Une personne qui exerce son droit d'accès doit obtenir la communication de l'intégralité des données qui la concernant, qu'elles soient stockées en base active ou archivées.

En santé : La conservation des données est réglementée, qu'il s'agisse des dossiers administratifs ou médicaux. Il faut faire la part entre l'archive vivante et active et le stockage long. Dans tous les cas, la sécurisation et la disponibilité de toutes les pièces est la règle.

Les bonnes questions à se poser :

- Jusqu'à quand ai-je vraiment besoin des données pour atteindre mon objectif ?

- Ai-je des obligations légales de conserver les données pendant un certain temps ?

- Dois-je conserver certaines données en vue de me protéger contre un éventuel contentieux ? Lesquelles ?

- Jusqu'à quand puis-je faire valoir ce recours en justice ?

- Quelles informations doivent être archivées ? Pendant combien de temps ?

- Quelles sont les règles de suppression des données.

- Quelles sont les règles d'archivage des données ?

En résumé :

Dois-je fixer une durée de conservation des données dans mon fichier ? **Oui**

Vous ne pouvez **pas conserver indéfiniment** des informations sur des personnes physiques dans vos fichiers. Si une durée de conservation n'est pas imposée par un texte légal (par exemple, 10 ans pour les documents comptables), il vous appartient de **fixer vous-même** cette durée en fonction de l'utilité de la donnée au regard du but poursuivi.

Attention : la durée de conservation des données que vous fixerez ne devra **pas être excessive** au regard des raisons pour lesquelles vous les avez collectées (par exemple, le temps de la relation contractuelle pour les informations figurant dans un fichier clients).

Au-delà de cette durée, vous devez **effacer** ou **anonymiser** les données.

TABLEAU INDICATIF DES DUREES DE CONSERVATION DES DONNEES

FINALITE DU TRAITEMENT	DUREE DE CONSERVATION
RESSOURCES HUMAINES	
Gestion du personnel	5 ans (en archivage intermédiaire) à compter du départ du salarié.
Gestion de la paie	5 ans à compter du versement de la paie
Fichiers de recrutement	Destruction immédiate si le candidat n'est pas retenu ni pour le poste à pourvoir ni dans le cadre d'un futur recrutement Possibilité de conserver le CV pendant 2 ans après le dernier contact avec le candidat
Vidéosurveillance	1 mois
Gestion des réunions instances représentatives du personnel	Les données relatives aux sujétions particulières ouvrant droit à congés spéciaux ou à un crédit d'heure de délégation ne sont pas conservées au delà de la période de sujétion de l'employé concerné
Gestion de l'annuaire du personnel	Les données ne sont pas conservées au delà de la période d'emploi de la personne concernée
Gestion des œuvres sociales et culturelles	Les données sont conservées tant que la personne travaille pour l'établissement ou jusqu'à ce qu'elle en demande la suppression
Contrôle de l'utilisation d'internet par les salariés	6 mois concernant l'historique des connexions
Contrôle de l'utilisation de la messagerie (outil de mesure de la taille, de la fréquence, analyse des pièces jointes, etc…)	6 mois
Gestion de la téléphonie (données relatives à l'utilisation des services de téléphonie : numéros appelés, numéros entrants, etc…)	1 an
Géolocalisation des véhicules professionnels	2 mois (historique des déplacements)
Contrôle des horaires	Les éléments d'identification ne doivent pas être conservés au delà de 5 ans après le départ du salarié. Les informations relatives aux horaires des salariés peuvent être conservées pendant 5 ans. La conservation des données relatives aux motifs d'absence est limitée à une durée de 5 ans
	En cas de paiement direct ou de prépaiement des repas les données monétique ne peuvent

Gestion de la restauration	pas être conservées plus de 3 mois. En cas de paiement par retenue sur salaire, la durée de conservation est de 5 ans.
Contrôle d'accès	Les éléments d'identification ne doivent pas être conservés au delà du temps pendant lequel la personne est habilitée à pénétrer dans les locaux concernés. 3 mois (historique des passages)
Sanctions disciplinaires	3 ans glissant sauf amnistie
Enregistrement des conversations téléphoniques	2 mois glissant
Autocommutateur (détail des appels téléphoniques)	6 mois glissant
Mandat des représentants des personnels (nature du mandat et syndicat d'appartenance)	6 mois après la fin du mandat
SANTE	
Dossier médical dans les cabinets libéraux	10 ans
Dossier médical dans les établissements de santé publics et privés	Conservation du dossier pendant 20 ans à compter du dernier passage (séjour ou consultation). Si la durées de conservation s'achève avant le 28ème anniversaire du patient, son dossier est conservé jusqu'à cette date. Si le patient décède moins de 10 ans après son dernier passage, le dossier est conservé pendant une durée de 10 ans après son décès.
Télétransmission des feuilles de soins	Conservation des doubles et AR pendant 90 jours
Gestion de la pharmacie, dispensation des médicaments, produits de santé, DM…	Conservation des données enregistrées sur le patient pendant 3 ans à compter de la dernière intervention sur son dossier. A l'issue de ce délai les données sont archivées pendant 15 ans. Conservation de l'ordonnancier pendant 10 ans. Conservation du registre des stupéfiants pendant 10 ans à partir de sa dernière mention. Conservation du registre des médicaments dérivés du sang pendant 40 ans.

Gestion des laboratoires d'analyse médicale	Conservation des données enregistrées sur le patient pendant 5 ans à compter de la dernière intervention sur son dossier. A l'issue de ce délai les données sont archivées pendant 10 ans. Pour les laboratoires en établissement de santé, conservation pendant 20 ans des dossiers et registres.
Recherche médicale	Détermination de la durée de conservation au cas par cas suivant le principe de proportionnalité. La durée de conservation est à déterminer en fonction de la finalité poursuivie et des catégories de données traitées. La durée de conservation doit être très courte, les données anonymisées ou pseudo anonymisées.
Analyse des pratiques ou des activités de soins et de prévention	Durée de conservation très courte, qui ne dépasse pas 2 ans dans la plupart des cas. Durée proportionnelle à la finalité de l'étude, conservée le temps de l'étude et supprimée dès la fin de l'étude.

LES MESURES DE SECURITE C'EST QUOI?

Les responsables d'un fichier et les sous-traitants doivent prendre toutes les mesures nécessaires pour assurer la sécurité et la confidentialité des données personnelles qu'ils traitent :

- Des mesures de sécurité physiques : sécurité des accès aux locaux ;
- Des mesures de sécurité informatiques : antivirus, sécurisation des mots de passe, etc.
- **Ils doivent également veiller à ce que seuls les destinataires autorisés puissent accéder aux données.**

A titre personnel au sein de l'établissement :

- Veillez à titre personnel à protéger toutes les données à caractère personnel auxquelles vous avez accès.
- Mettez en place des codes d'accès complexes pour vos applications : mot de passe à 15 caractères incluant des chiffres, lettres, majuscules et minuscules et caractères spéciaux (exemple : **%AndertY137I9%*)** et changez vos codes d'accès régulièrement.
- N'affichez pas vos codes sur le PC avec un postit, ne les stockez pas sur un fichier word ou excel, ni sur un document papier.
- N'ouvrez pas de mail dont vous ne connaissez pas formellement l'émetteur et ne cliquez que sur des liens non authentifiés.
- Ne transmettez aucun fichier de données par la messagerie personnelle ou celle de l'établissement ou encore Gmail ou téléphonie mobile. Ces messageries ne sont pas sécurisées.
- Utilisez la messagerie **MS-SANTE** ou **APICRYPT**.
- Ou cryptez le fichier transmis avec **7Zip** ou **VERA CRYPT** (recommandés par la CNIL et l'ANSI) avant transfert.
- Ne laisser pas trainer des données stockées sur un disque externe (clef USB ou DD externe) sans les crypter.
- Crypter les données si vous les exploitez sur un PC personnel.
- **D'une façon générale, avant de stocker des données nominatives, évaluez la pertinence de conserver la part nominative de ces données**, sinon **ANONYMISEZ** les.
- **ATTENTION aux logiciels trouvés sur le web ou délivrés par les labos.**
- Retenez que tout traitement de données nominatives doit être déclaré au DPO ou au RIL (responsable informatique et liberté) de l'établissement selon des modalités qu'il vous expliquera, et être intégré au **REGISTRE** des données de l'établissement.
- Tout traitement de données personnelles doit faire l'objet d'un accord écrit des personnes concernées.
- La CNIL est en droit, sur contrôle systématique ou plainte, d'effectuer un contrôle dans l'établissement, avec la prise de sanctions administratives (suspension de l'autorisation de traitement), pénales, et financières très lourdes (jusqu'à 20 millions d'Euros).
- Informez vos internes, étudiants et collaborateurs de ces obligations, en particulier lors de leurs travaux de publications, mémoires et thèses.

- Soyez prudents lors de vos activités de recherche, lors de la saisie en ligne de données patients….le site est-il sécurisé, et comment ?...n'oubliez pas que le web est un grand marché…
- Toute fuite, perte, tout piratage doivent être notifiés au RSSI de l'établissement pour mise en œuvre de mesures de sécurisation, déclaration à l'autorité de contrôle et information aux personnes concernées.

ANONYMISER LES DONNEES, C'EST QUOI?

Anonymisation

L'anonymisation est une opération qui consiste à transformer des données personnelles afin de ne plus permettre l'identification de la personne concernée. Cette transformation doit être **irréversible**. C'est-à-dire qu'il ne doit pas exister de méthode directe ou indirecte permettant de rattacher les données à la personne d'origine.

Les données comportant des informations à caractère personnel peuvent être conservées au-delà des délais de détention autorisées par la CNIL si elles sont convenablement anonymisées.

Cette technique est nécessaire pour transmettre tout ou partie du jeu de données à un tiers qui a besoin de travailler sur les données réelles sans avoir besoin des données nominatives.

Une donnée anonyme n'est plus une donnée à caractère personnel…donc elle sort du champ d'application de la loi et les personnes concernées n'ont plus de droits à faire valoir….MAIS le processus d'anonymisation étant un traitement de données à caractère personnel, il doit être déclaré.

L'anonymisation est correcte s'il n'est pas possible :

- D'isoler ou d'individualiser des informations relatives à un seul individu
- De relier ou corréler les données d'un individu à un groupe d'individu
- De déduire ou d'interférer d'un ensemble d'attributs la valeur d'un autre attribut.

Quelques méthodes d'anonymisation à combiner:

- Ajout de bruit : altérer la justesse de l'information en introduisant un aléa cohérent (exemple : intégrer des noms de ville sans lien avec l'identité)
- Permutation : mélanger les valeurs d'attribut au sein du jeu de données
- Généralisation : changer la granularité des valeurs pour former des groupes (exemple : intégrer des tranches d'IMC)
- Substitution
- Renumérotation
- Hachage ou chiffrement
- Suppression définitive d'un attribut (une colonne)

Pseudonymation

Il arrive parfois qu'on veuille rendre les données personnelles illisibles tout en conservant la possibilité de lever le secret. L'anonymat étant, en toute rigueur, irréversible, on parle dans ce cas de pseudonymat.

ALORS, LE RGPD C'EST QUOI ?

Les dispositions générales

L'objectif est de protéger les données à caractère personnel de **traitements automatisés en tout ou partie ou de traitements non automatisés.**
Cette réglementation concerne le territoire de l'Union Européenne et tout territoire sur lequel un établissement participe à la collecte des données.

Les principes

- **Le traitement des données à caractère personnel doit-être** licite, loyal et transparent.
- Les données doivent être collectées pour des **finalités déterminées**, **adéquates, pertinentes** et **limitées** aux **finalités déterminées**. De plus, elles doivent être **exactes** ou tenue à jour, **conservées** le temps nécessaire et identifiables pour chaque individu concerné et surtout **protégées** contre un traitement non autorisé.
- **En ce qui concerne la licéité du traitement**, l'établissement doit obtenir le **consentement** de la personne concernée si elle est âgée d'au moins **16 ans** ou le consentement du titulaire de la responsabilité de la personne si l'âge est inférieur à 16 ans.
- **Le traitement doit obligatoirement participer** à **l'exécution d'un contrat**, au **respect d'obligation légale**, aux **intérêts vitaux de la personne** concernée, à **l'exécution d'une mission d'intérêt public** et aux fins **d'intérêts légitimes** poursuivis par le responsable du traitement.
- **Le consentement de la personne concernée** impose que le **responsable du traitement** soit en mesure de **démontrer la preuve** de la personne concernée. La **personne** a le **droit de retirer son consentement** à tout moment et le **responsable du traitement** doit **informer clairement** la personne concernée si l'exécution d'un contrat **nécessite le traitement de données** à caractère personnel.
- **Les données suivantes sont interdites dans les traitements**, notamment si le consentement et la licéité ne sont pas démontrés. Le responsable du traitement et les sous-traitants ne doivent en aucun cas traiter les données concernant l'origine **raciale** ou **ethnique**, les **opinions politiques**, les convictions **religieuses** ou **philosophiques**, l'appartenance **syndicale**, l'**orientation sexuelle**, les **données génétiques**, **biométriques** et les **condamnations pénales et les infractions**.

Les droits de la personne concernée

Le **responsable du traitement** (Chef d'établissement) prend des **mesures appropriées** pour fournir en toute transparence toute les Informations demandées par les personnes concernées :

- Droit d'accès
- Droit d'opposition
- Droit de rectification
- Droit à l'effacement (« droit à l'oubli »)
- Droit à la limitation de traitement
- Droit à la portabilité des données

Le responsable du traitement (Chef d'établissement) doit fournir un accès aux informations suivantes :

- identité et coordonnées du responsable ou du représentant du traitement
- coordonnées du délégué à la protection des données
- les finalités et la base juridique du traitement
- les destinataires du traitement
- la durée de conservation
- l'existence d'une prise de décision automatisée y compris l'usage de profilage.

La **personne concernée** a également le **droit de ne pas faire l'objet** d'un traitement automatisé et le **responsable du traitement** doit tout mettre en œuvre pour **préserver les droits et libertés** de la personne concernée par un traitement automatisé.

Cependant, les droits individuels peuvent être ouverts dans les situations suivantes :

- Sécurité nationale
- Défense nationale
- Sécurité publique
- Préventions et détections d'infractions
- Intérêts publics
- Indépendance de la justice
- Respects des professions réglementées
- Mission de contrôle
- Protection des droits et libertés d'autrui
- L'exécution des demandes de droit civil

Les obligations du responsable du traitement

Ils doivent mettre en œuvre toutes mesures pour être conforme à la réglementation au niveau organisationnel et technique.
La protection des données à caractère personnel doit être prise en compte ***dès la conception des traitements (Privacy by design).***

Il s'agit d'effectuer systématiquement avant toute mise en œuvre d'un nouveau traitement (mais aussi pour les traitements déjà existants), une analyse des risques a priori et de mettre en place les mesures de protection préventives.

Les sous-traitants

Les sous-traitants doivent garantir qu'ils respectent le RGPD. Il convient donc de recenser tous les sous-traitants et de modifier les clauses contractuelles et ils doivent préciser leur engagement.

Nomination d'un DPO

Le responsable du traitement et les sous-traitants doivent obligatoirement nommer un **responsable de la protection des données** (DPO). Ce DPO peut être mutualisé ou externalisé. Il est indépendant.

Tenue d'un registre

Le responsable du traitement doit tenir un REGISTRE des activités des traitements effectués et intégrer :

- le nom et les coordonnées du responsable du traitement et, le cas échéant, du responsable conjoint du traitement, du représentant du responsable du traitement et du délégué à la protection des données
- les finalités du traitement
- une description des catégories de personnes concernées et des catégories de données à caractère personnel
- les catégories de destinataires auxquels les données à caractère personnel ont été ou seront communiquées, y compris les destinataires dans des pays tiers ou des organisations internationales
- le cas échéant, les transferts de données à caractère personnel vers un pays tiers ou à une organisation internationale, y compris l'identification de ce pays tiers ou de cette organisation internationale ainsi que, les documents attestant de l'existence de garanties appropriées
- dans la mesure du possible, les délais prévus pour l'effacement des différentes catégories de données
- dans la mesure du possible, une description générale des mesures de sécurité techniques et organisationnelles.

Charte ou Code de conduite

L'Etablissement doit formaliser et diffuser un ***Code de conduite ou une Charte***. Ce document doit aborder et répondre aux points suivants :

- le traitement *loyal et transparent* des données à caractère personnel
- décrire les *intérêts légitimes* poursuivis par les responsables du traitement dans des contextes spécifiques
- décrire comment est effectuée la *collecte des données* à caractère personnel
- la méthode utilisée pour la *pseudonymisation des données* à caractère personnel
- quelles sont les *informations communiquées* au public et aux personnes concernées
- comment est régit *l'exercice des droits* des personnes concernées
- qu'elles sont les *informations communiquées aux enfants* et la protection dont bénéficient les enfants et la manière d'obtenir le *consentement des titulaires* de la responsabilité parentale à l'égard de l'enfant
- la gestion des *mesures et des procédures* visant à assurer la sécurité du traitement
- la procédure mise en œuvre pour émettre la *notification aux autorités de contrôle* des violations de données à caractère personnel et la communication de ces violations aux personnes concernées
- la procédure de *transfert de données* à caractère personnel vers des *pays tiers* ou à des organisations internationales
- les *procédures extrajudiciaires* et autres procédures de règlement des litiges permettant de résoudre les litiges entre les responsables du traitement et les personnes concernées en ce qui concerne le traitement
- décrire le mécanisme de *certification* mis en œuvre éventuellement par le responsable de traitement ou du sous-traitant

- la procédure utilisée pour *répondre aux autorités de contrôle*
- les règles adoptées pour la *sécurité des traitements*, notamment:
- la *pseudonymisation et le chiffrement des données* à caractère personnel
- les moyens permettant de garantir la *confidentialité, l'intégrité, la disponibilité et la résilience constantes* des systèmes et des services de traitement
- les moyens permettant de rétablir la *disponibilité des données* à caractère personnel et l'accès à celles-ci dans des délais appropriés en cas d'incident physique ou technique
- la procédure visant à *tester, à analyser et à évaluer régulièrement* l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement.
- la procédure pour *notifier dans les 72 h les autorités de contrôle* en cas de violation
- la procédure pour *notifier dans les 72 h les personnes concernées* par le cas de violation
- Mettre en place les éléments et les personnes apte à faire une analyse d'impacts au *niveau corporels, matériels et moraux.*

Information

Il convient de recenser tous les supports d'information (livret d'accueil, site web, documents délivrés aux patients…) et d'y intégrer les informations réglementaires liées au RGPD.

De même l'établissement doit organiser des sessions d'informations ouvertes sur le RGPD.

Les transferts des données

Le responsable de traitement peut effectuer des transferts de données à caractère personnel s'ils sont fondés sur une **décision d'adéquation** respectant **l'Etat** de **droit**, **le Respect** des **droits de l'homme** et des **libertés fondamentales** et **l'Existence** d'autorités de **contrôle**. Cela concerne sans problème l'UE.

Le responsable doit s'assurer de l'existence de garanties appropriées, telles que des **accords** entreprises, internationaux et des accords de **coopération internationale** dans la protection des données à caractère personnel.

Les transferts de données avec les USA ne peuvent être systématisés et doivent faire l'objet d'une analyse au cas par cas selon les entreprises.

Autorités de contrôle : CNIL en France

Les autorités de contrôle sont implantées dans chaque pays et **indépendantes** (la CNIL en France). Elles sont regroupées pour coopérer ensemble au sein du G29. Elles se doivent assistance mutuelle et organisent des opérations conjointes.

Parmi ses missions, la CNIL contrôle l'application du RGPD, veille au respect de celui-ci, favorise la sensibilisation du public, conseille les dirigeants du pays, fournit, sur demande, à toute personne concernée des informations sur l'exercice des droits que lui confère le règlement, traite les réclamations introduites par une personne concernée ou par un organisme, une organisation ou une association, et informe l'auteur de la réclamation de l'état d'avancement et de l'issue de l'enquête, effectue des enquêtes sur l'application du règlement, y compris sur la base d'informations reçues d'une autre autorité de contrôle ou d'une autre autorité publique, s'acquitte de toute autre mission relative à la protection des données à caractère personnel….

La CNIL exerce les pouvoirs suivants :

- ordonner au responsable du traitement et au sous-traitant, et, le cas échéant, au représentant du responsable du traitement ou du sous-traitant, de lui communiquer toute information dont elle a besoin pour l'accomplissement de ses missions
- mener des enquêtes sous la forme d'audits sur la protection des données
- procéder à un examen des certifications délivrées en application de l'article 42, paragraphe 7
- notifier au responsable du traitement ou au sous-traitant une violation alléguée du présent règlement
- obtenir du responsable du traitement et du sous-traitant l'accès à toutes les données à caractère personnel et à toutes les informations nécessaires à l'accomplissement de ses missions
- obtenir l'accès à tous les locaux du responsable du traitement et du sous-traitant, notamment à toute installation et à tout moyen de traitement, conformément au droit de l'Union ou au droit procédural des États membres.

Voies de recours et sanctions

La loi prévoit le droit d'introduire une **réclamation** auprès de la CNIL ou un **recours juridictionnel** effectif contre un responsable du traitement, un sous-traitant. Cette action peut être individuelle ou collective.

La CNIL peut demander des explications auprès du responsable du traitement, ou effectuer un contrôle. Elle peut imposer des sanctions : injonction, arrêt de traitement, amendes administratives pouvant s'élever jusqu'à **20 000 000 €** ou, dans le cas d'une entreprise, jusqu'à **4 % du chiffre d'affaires annuel mondial** total de l'exercice précédent.

EN RESUME :

Pertinence des données collectées	Nomination d'un DPO
Droit des personnes	Tenue d'un registre
Cartographie des traitements	Régularisation des sous traitants
Privacy by design	Information

LES POINTS DE VIGILANCE A RETENIR

Dans le monde hospitalier, sont concernés les patients et les professionnels.

L'esprit de la loi est de protéger les données personnelles et donc la vie privée de tous.

Chacun a le droit d'accéder à ses données collectées…et donc à l'intégralité de son dossier médical ou administratif.

Tout refus ou différé est condamnable, peut légalement justifier de plaintes et donc faire l'objet de sanctions pénales et administratives.

Certains secteurs sont particulièrement sensibles :

- les RH
- les surveillances : video surveillance, badges d'accès
- la confidentialité des dossiers administratifs et médicaux
- les activités de recherche
- les transferts d'information (mail, fax…)
- les « fichiers cachés » à usage interne…

Il vous est donc recommandé de lier la protection des données personnelles au sens de la loi, à votre forte implication dans la garantie de la sécurité des données collectées.

Pour toute question, n'hésitez pas à vous rapprocher du DPO ou du RSSI de votre établissement.

LES BONS LIENS À CONNAITRE C'EST …..?

https://www.ssi.gouv.fr/

https://www.cyberveille-sante.gouv.fr/

https://www.cnil.fr/