LE RÈGLEMENT GÉNÉRAL SUR LA PROTECTION DES DONNÉES

« LES PRINCIPES APPLICABLES AU SECTEUR DE LA SANTÉ »

RÉSUMÉ

La protection des données de santé a beaucoup évolué en quelques années.

Le Règlement vient aujourd'hui entériner une **définition** précise des données de santé, tant qu'un niveau de protection adéquat.

Les acteurs impliqués dans les sciences de la vie doivent donc connaître un certain nombre de **principes de protection**, pour les transformer rapidement en réflexe dès la conception d'un projet.

De plus, les personnes concernées par les données traitées ont désormais plus de **pouvoir sur « leurs informations »**, mais il n'est pas pour autant question d'une propriété des données au sens juridique ; il est important de maîtriser ces principes de droit, de manière à répondre correctement à ses interlocuteurs et prévenir d'éventuels contentieux.

RAPPEL DES BASES DU RGPD

- **Arrivée du RGPD, 40 ans après la loi informatique et libertés…**
  - Dans les années 70, des inquiétudes sur l'automatisation des fichiers se font entendre… « *La dynamique du système qui tend à la centralisation des fichiers risque de porter gravement atteinte aux libertés, et même à l'équilibre des pouvoirs politiques* » (Le Monde, Pierre Boucher, « *Safari* ou la chasse aux français », 1973).
    SAFARI avait pour objectif l'interconnexion des fichiers administratifs à partir du numéro de Sécurité sociale. Suite à l'émoi provoqué, le Premier ministre demande la constitution d'une commission « Informatique et Libertés ».
  - 5 ans plus tard, la **loi relative à l'informatique, aux fichiers et aux libertés du 6 janvier 1978** est adoptée et sera à l'origine de la protection des données en Europe
  - L'Union européenne décide de protéger les données personnelles sur son territoire : la **Directive de 1995** s'inspire fortement de la loi française.
  - La Directive n'est transposée en France qu'avec la l**oi de 2004 qui modifie la législation "Informatique et Libertés"**. Elle renforce le dispositif pénal en son sein et qualifie de *sensibles* les données de santé.
  - Le **RGPD** est adopté le 14 avril 2016, directement applicables à compter du 25 mai 2018 dans l'ensemble des 28 États membres de l'Union européenne
  - **En France,** le projet de loi relatif à la protection des données vise à « suradapter » le droit français au RGPD. Au Parlement, les discussions sont âpres sur certaines questions à adapter en droit français (chiffrement comme méthode de sécurisation, âge des mineurs pouvant consentir, responsabilités des collectivités territoriales, etc.)

RAPPEL DES BASES DU RGPD

- **Champs d'application**
  - Territoire de l'union européenne

    - Sociétés établies dans l'UE
    - Sous-traitants établis dans l'UE
    - Personnes concernées par le traitement dans l'UE

  - Personnes physiques et non personnes morales :
    le règlement « *ne couvre pas les traitements des données à caractère personnel qui concernent les personnes morales et en particulier des entreprises dotées de la personnalité juridique, y compris le nom, la forme juridique et les coordonnées de la personne morale.* » (cons. 14)
    Le règlement ne vise donc qu'à protéger les personnes physiques.

LES POINTS ESSENTIELS

- **Le caractère « personnel » de la donnée**
- **Le caractère « sensible » de la donnée**
- **Les conditions pour les traitements de données de santé**

1. Consentement
2. Sécurité
3. Transparence

DÉFINITION DE LA DONNÉE A CARACTÈRE PERSONNEL

Comme l'énonce son intitulé complet, le RGPD s'applique aux traitements de données à caractère personnel.

Tout l'enjeu est donc de savoir ce que recouvre la notion de traitement et ce que recouvre la notion de données à caractère personnel.

Donnée à caractère personnel : « *Toute information se rapportant à une personne physique identifiée directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale* ». Art 4.1 RGPD

… Concrètement une donnée à caractère personnel, qu'est-ce que c'est ?

DÉFINITION DE LA DONNÉE DE SANTÉ

Les **données à caractère personnel concernant la santé** devraient comprendre, en particulier, l'ensemble des données se rapportant à l'état de santé d'une personne concernée;

les informations relatives à l'enregistrement du patient pour la prestation de services de santé;

les informations relatives aux paiements ou à l'éligibilité du patient à des soins de santé;

un numéro ou un symbole attribué à un patient, ou des informations détaillées le concernant, destinés à l'identifier de manière univoque à des fins médicales;

toute information relative au patient recueillie dans le cadre de la prestation de services de santé audit patient;

des informations obtenues lors d'un contrôle ou de l'examen d'un organe ou d'une substance corporelle, y compris des échantillons biologiques;

l'identification d'une personne en tant que prestataire de soins de santé au patient;

ou toute information concernant, par exemple, une maladie, un handicap, un risque de maladie, un dossier médical, un traitement clinique ou l'état physiologique ou biomédical de la personne concernée, indépendamment de sa source, qu'elle provienne par exemple d'un médecin ou d'un autre professionnel de la santé, d'un hôpital, d'un dispositif médical ou d'une épreuve diagnostique in vitro.

LE RÉGIME DE LA DONNÉE DE SANTÉ

Conséquence : interdiction par principe, autorisation par dérogation

- Le RGPD, comme la loi I&L prévoit une interdiction :
  – des traitements des données à caractère personnel qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi que les traitements des données concernant **la santé** ou la vie sexuelle d'une personne physique,
  - Les traitements des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique.

- La **licité** du traitement de données repose sur le **consentement** de la personne concernée, la **sécurité** et la **transparence** !

1. LE CONSENTEMENT ET LE DROIT DES PERSONNES

- **Le consentement de la personne**
  - Fin de l'opt-out et du consentement présumé de la loi santé de 2016…
  - Traçabilité du recueil de consentement
  - Validité du consentement subordonnées à l'information

1. LE CONSENTEMENT ET LE DROIT DES PERSONNES

- **Le droit des personnes concernées**
  - Droit à rectification, effacement, verrouillage, limitation des données inexactes ou incomplètes, ou quand les données ne sont plus nécessaires à la finalité du traitement ou qu'elles sont illicites (Dir. 95)
  - Droit à la portabilité (NEW!)
  - Droit d'opposition présenté distinctement des autres droits (NEW!)
  - Droit de ne pas faire l'objet d'une décision individuelle automatisée sauf si cela est nécessaire à un contrat ou avec le consentement (NEW!)

2. LA SÉCURITÉ

- Article 32
- Les responsables de traitements et leurs éventuels sous-traitants ont l'obligation de « garantir un niveau de sécurité adapté au risque ».
- Pseudonymisation* ou chiffrement des données à caractère personnel, et adoption de « moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement ».
    - La crypto : Amendement sénat
      Les sénateurs ont adopté un amendement visant à contraindre les responsables de traitement de données personnelles à les chiffrer « *chaque fois que cela est possible* » (Voir art. NextInpact)
    - Or refus du Gouvernement et de l'Assemblée
      QPC sur l'article 434-15-2 du Code pénal => Décision du 30 mars du Conseil constitutionnel.

*Pseudonymisation : données perso !

3. LA TRANSPARENCE

- Déclarer ses sous-traitants / Travailler avec le responsable de traitement
  - Déclarer la sous-traitance (NB. Marque blanche..)
  - Contrats écrits avec clauses spécifiques (dès l'appel d'offre pour les pers. publiques)
  - Si le sous-traitants n'est pas dans l'UE, désigner un représentant sur le territoire
  - Le sous-traitant doit documenter ses procédures et appliquer un code de conduite
- Cartographier ses responsabilités avec un outil de PAI
- Obtenir une certification traduisant la conformité au RGPD

CONCLUSION

En santé, beaucoup de précautions définies par le RGPD existaient déjà !

- Recueil du consentement pour les données de santé depuis 1995
- L'information du patient : livret d'accueil dans les établissements, contrat de séjour, document de prise en charge, formulaire de recueil de consentement, …
    - Depuis 2002, « Loi Kounchner », « Loi 2002-2 », …
    - Depuis 2012, pré-requis du programme hôpital numérique (P/3)…
- Transparence sur la sous-traitance : la PGSSI-S imposait déjà de référencer ses partenaires (la Loi santé du 26 janvier 2016 prévoit l'opposabilité des référentiels de la PGSSI-S).
- La procédure de signalement des incidents de sécurité est prévu par le décret du 12 septembre 2016
- Le DPO est un CIL bien formé ! (obligation de désigner un DPO pour les responsable de traitement dont la santé est l'activité de base et pour les traitements à grande échelle)

Merci !

Caroline ZORN
Avocate - Docteure en droit
contact@warp-avocats.eu

9 place Haguenau
F-67000 STRASBOURG
+333 67 10 69 80