DE GAULLE
FLEURANCE
& ASSOCIÉS

SOCIÉTÉ D'AVOCATS

La protection des données à caractère personnel à la lumière du RGDP
Hébergement des données de santé

INTERMEDITECH

16 mai 2017

Jean-Marie Job

avocat associé

DE GAULLE FLEURANCE & ASSOCIÉS
SOCIÉTÉ D'AVOCATS

La donnée personnelle est au cœur des dispositifs médicaux

- Au stade du développement si le dispositif médical doit faire l'objet d'essais cliniques
- Les logiciels embarqués dans les dispositifs médicaux
- Les dispositifs médicaux connectés et les projets *big data* associés
- Les App santé lorsqu'elles sont des dispositifs médicaux

DE GAULLE FLEURANCE & ASSOCIÉS
SOCIÉTÉ D'AVOCATS

Un cadre juridique en pleine évolution

En Europe

- **Le Règlement général sur la protection des données – 27 avril 2016**

Applicable le 25 mai 2018

En France

- **Loi santé du 26 janvier 2016 :** modifications de la loi Informatique et libertés (données liées à la recherche – Système National des Données de Santé)
- **Ordonnance Recherche 16 juin 2016**
- **Décret du 26 décembre 2016** (application de la Loi informatique et libertés et SNDS)
- **Ordonnance 12 janvier 2017** hébergement des données de santé

DE GAULLE FLEURANCE & ASSOCIÉS
SOCIÉTÉ D'AVOCATS

Les fondamentaux – définitions du RGDP

- **Donnée à caractère personnel**

Toute information se rapportant à une personne physique identifiée ou identifiable (ci-après dénommée «personne concernée»); est réputée être une «personne physique identifiable» une personne physique qui peut être 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

- **Traitement de données**

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, telles que 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;

- **Responsable de traitement**

La personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement

- **Sous-traitant**

La personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement

DE GAULLE FLEURANCE & ASSOCIÉS
SOCIÉTÉ D'AVOCATS

Champ d'application du RGDP

- Matériel
  - « *Traitement de données à caractère personnel, automatisé en tout ou en partie ET traitement non automatisé de données à caractère personnel contenues ou appelées à figurer dans un fichier* » (article 2)
- Territorial : élargissement (article 3)
  - Traitement de données à caractère personnel (DCP) dans le cadre des activités d'un établissement, d'un responsable du traitement (RT) ou d'un sous-traitant (ST) établi sur le territoire de l'UE (même si le traitement se fait hors UE)
  - Traitement des DCP sur des personnes se trouvant sur le territoire de l'UE par un RT ou un ST qui n'est pas établi dans l'Union, lorsque les activités de traitement sont liées :
    - à l'offre de biens ou de services (avec ou sans paiement exigé)
    - au suivi du comportement, ayant lieu au sein de l'UE, des personnes concernées
  - Traitement de DCP par un RT établi hors UE mais dans un lieu où le droit d'un État membre s'applique en vertu du droit international public

DE GAULLE FLEURANCE & ASSOCIÉS
SOCIÉTÉ D'AVOCATS

Principes et conditions de licéité des traitements

Rappel ou nouveaux principes relatifs au traitement de DCP (art. 5)

- Licéité, loyauté et **transparence**
- Limitation des finalités
- Minimisation de données
- Exactitude
- Limitation de la conservation
- Intégrité et confidentialité
- Responsabilité

Licéité du traitement de DCP (art. 6)

Le traitement doit reposer sur l'un des fondements limitativement énumérés par le RGDP

- Consentement
- Exécution d'un contrat
- Respect d'une obligation légale imposée au responsable du traitement
- Sauvegarde des intérêts vitaux
- Exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement
- Intérêts légitimes poursuivis par le RT ou par un tiers (exceptions)

DE GAULLE FLEURANCE & ASSOCIÉS
SOCIÉTÉ D'AVOCATS

Le renforcement des droits des personnes

1. **Encadrement renforcé du consentement** (+ focus enfants) (art. 7)
2. **Transparence** (nouveau principe) (art. 12)
3. Information et droit d'accès
4. Rectification et effacement
   - Rectification (art. 16)
   - **Droit à l'oubli** (art. 17)
   - **Droit à la limitation du traitement** (art. 18)
   - Notification des rectifications/effacement (art. 19)
   - **Portabilité des données** (art. 20)
5. Droit d'opposition et décision individuelle automatique/ **profilage**
6. Droit à un recours juridictionnel effectif et **droit à réparation** (art. 77 et suiv.)

DE GAULLE FLEURANCE & ASSOCIÉS
SOCIÉTÉ D'AVOCATS

Les acteurs du traitement

Responsable de traitement (art. 24)

Mise en œuvre des mesures techniques/organisationnelles appropriées pour s'assurer et être en mesure de démontrer que le traitement est effectué conformément au RGDP :

- **Privacy by design:** Protection des données dès la conception et protection des données par défaut (pseudonymisation, minimisation des données)
- **Garantir la protection des droits des personnes reconnus par le RGDP** (transparence, droit à l'oubli, limitation, portabilité…) (art. 25)
- **Tenue d'un registre** (art. 30)
- **Garantir la sécurité technique du traitement en fonction des risques de chaque traitement** (art. 32)
- **Notification des violations DCP** (art. 33)
- **Réalisation d'analyses d'impact sur la protection des données** (art. 35)
- **Désignation d'un DPO** (art. 37)
- **Code de conduites et certification** – facultatif (art. 40 et 42)

- RT doit vérifier et garantir que le ST respecte le RGDP

Possibilité de responsables conjoints (art. 26)

Un ou plusieurs RT déterminent conjointement les finalités et moyens du traitement

Accord définissant les rôles respectifs

Mêmes obligations que les RT

DE GAULLE FLEURANCE & ASSOCIÉS
SOCIÉTÉ D'AVOCATS

Les acteurs du traitement

Sous-Traitant (art. 28)

- **Présente des garanties suffisantes (mesures techniques et organisationnelles)**
- **Pour recrutement d'un autre ST: Autorisation écrite et préalable du RT**
- **<u>Contrat</u> sous-traitant: obligations minimales (action sur instruction RT, confidentialité, aide RT à respecter dispositions liées à la notification/communication des violations et analyses d'impact)**
- **Code de conduite ou mécanisme de certification possible**
- **Tenu d'un registre (art. 30)**
- **DPO**
- **Clauses contractuelles types**
- **ST tombe sous la qualification de RT s'il détermine les finalités et moyens du traitement (en violation du RGDP)**

DE GAULLE FLEURANCE & ASSOCIÉS
SOCIÉTÉ D'AVOCATS

Accountability

Une responsabilisation contre moins de formalités dès lors que la conformité peut être démontrée

Quels outils pour cette démonstration ?

- Registre
- Notifications de violations
- Codes de conduite et certifications
- DPO
- Analyses d'impact

Suppression des obligations déclaratives (formalités possibles pour données sensibles)

DE GAULLE FLEURANCE & ASSOCIÉS
SOCIÉTÉ D'AVOCATS

Les données de santé

Données sensibles/ données de santé (Article 9 : données de santé et données génétiques)

- *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 (article 4.15))*

- *données à caractère personnel relatives aux caractéristiques génétiques héréditaires ou acquises d'une personne physique qui donnent des informations uniques sur la physiologie ou l'état de santé de cette personne physique et qui résultent, notamment, d'une analyse d'un échantillon biologique de la personne physique en question (article 4.13))*

➢ **Principe: interdiction de collecter les données sensibles**

➢ **Exceptions:**

- Consentement
- Motif d'intérêt public dans le domaine de la santé publique
- Médecine préventive, curative, gestion des systèmes de santé/protection sociales :

« *le traitement est nécessaire pour des motifs d'intérêt public dans le domaine de la santé publique, tels que la protection contre les menaces transfrontalières graves pesant sur la santé, ou aux fins de garantir des normes élevées de qualité et de sécurité des soins de santé et des médicaments ou des dispositifs médicaux, sur la base du droit de l'Union ou du droit de l'État membre qui prévoit des mesures appropriées et spécifiques pour la sauvegarde des droits et libertés de la personne concernée, notamment le secret professionnel* » (Art. 9.2.i)

- (…)

Les données de santé

- **Dérogations aux traitements nécessaires à des fins de recherche scientifique** (art. 89)

  - ✓ Respecter l'exercice du droit à la protection
  - ✓ Prévoir des mesures appropriées pour assurer le respect du principe de minimisation
  - ✓ Privilégier la pseudonymisation
  - ✓ Possibilité de déroger aux droits d'accès, rectification , limitation et opposition

Les données de santé

- **La subsidiarité : données de santé**

« *Les États membres peuvent maintenir ou introduire des conditions supplémentaires, y compris des limitations, en ce qui concerne le traitement des données génétiques, des données biométriques ou des données concernant la santé* » (art. 9.4)

Le maintien en vigueur de certaines dispositions de la Loi Informatique et Libertés est-il possible/ probable?

- L'article 8-III de la Loi Informatiques et Libertés
- Le chapitre IX de la Loi Informatiques et Libertés

DE GAULLE FLEURANCE & ASSOCIÉS
SOCIÉTÉ D'AVOCATS

Les nouveautés en matière d'hébergement des données de santé

Ordonnance du 12 janvier 2017

- Prestations d'hébergement, rôles / responsabilités de l'hébergeur, stipulations du contrat d'hébergement, conditions délivrance des certificats : fixés par décret en CE

- **Agrément** hébergement DP sur support numérique=> certificat de conformité (ISO) délivré par organisme accrédité (agrément pour la conservation DPS support papier ou l'archivage sur support numérique)

- **Entrée en vigueur** fixée par décret et au 1er janvier 2019 maximum (dispositions transitoires – délai minimum de mise en conformité pour agréments prenant fin dans les 12 mois après application nouveau régime)

DE GAULLE FLEURANCE & ASSOCIÉS
SOCIÉTÉ D'AVOCATS

Entrée en vigueur du RGDP 25/05/2018

Méthodologie de travail

- Inventaire et analyse des traitements concernés
  - Identification des traitements
  - Statut au regard des obligations LIL
  - Ecarts RGDP
- Audits informatique / sécurité
- Désignation ou non d'un DPO
  - obligatoire ou non
  - Avantages/inconvénients
- Préparation registres
- Réalisation ou non d'analyses d'impact
- Intégration du privacy by design
- Adaptation contrats/formulaires d'informations
- Adaptation procédures internes

Sensibilisation :
DG
CoDir

Création :
Equipe projet

DE GAULLE
FLEURANCE
& ASSOCIÉS
SOCIÉTÉ D'AVOCATS

Merci de votre attention

Jean-Marie Job : jmjob@dgfla.com

De Gaulle Fleurance & Associés
9 rue Boissy d'Anglas – 75008 Paris – France – Tél.: +33 (0)1 56 64 00 00 – Fax.: +33 (0)1 56 64 00 01
222 avenue Louise – 1050 Bruxelles – Belgique – Tél.: +32 (0)2 644 01 64 – Fax.: +32 (0)2 644 31 16
www.degaullefleurance.com