DESMARAIS AVOCATS

42ème Congrès FEHAP
22 & 23 NOVEMBRE 2017 À CLERMONT-FERRAND
LE PRIVÉ NON LUCRATIF EN MOUVEMENT
SPORT·INCLUSION·SANTÉ·BIEN-ÊTRE
CAP SUR LA PRÉVENTION

Les grands principes du RGPD

42ème Congrès de la FEHAP

34, rue Pétrelle • 75009 PARIS
contact@desmarais-avocats.fr • www.desmarais-avocats.fr

Une utilisation responsable des données

- Le RGPD n'est pas un frein au traitement des données
  - Mieux, dans certains cas, il le facilite (ex: intérêt légitime du responsable, données pseudonymisées, etc.)

- Le RGPD, c'est un changement de paradigme
  - Traditionnellement, volonté de contrôle a priori du fait d'une méfiance à l'égard des traitements de données
  - L'entrée dans les mœurs des traitements de données conduit à une logique de responsabilisation, « *à l'anglo-saxone* »

- Le RGPD promeut un marché de la donnée personnelle, sous réserve d'une utilisation raisonnable de cette *marchandise*

La détermination du périmètre de la notion de

« *Donnée de santé* »

Donnée personnelle, donnée de santé: késako?

- Données à caractère personnelle:
  - Toute donnée relative à une personne physique identifiée ou **raisonnablement** identifiable

- Données relatives à la santé
  - Toute donnée relative à la santé physique ou mentale, y compris la prestation de services de soins de santé, qui révèlent des informations sur l'état de santé de cette personne
  - Comprend notamment:
    - Toute donnée « *indépendamment de sa source* » ➔ L'IoT produit des données de santé
    - Donnée médico-administrative ➔ Le NIR est une donnée de santé
    - Donnée relative au handicap ➔ Le médico-social entre dans la sphère des données de santé

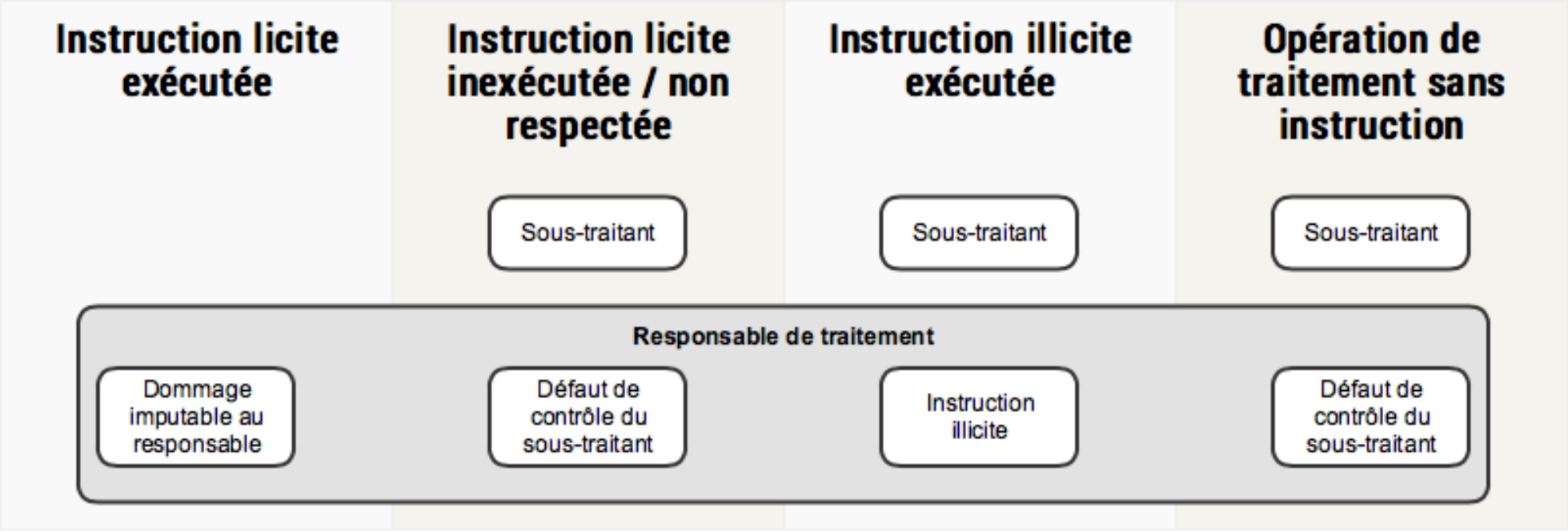
Des acteurs responsables

La responsabilisation des acteurs

- Outre les personnes concernées, 2 types d'acteurs:
  - Le responsable de traitement
  - Le sous-traitant (pas de responsabilité directe, aujourd'hui)
- Le RGPD responsabilise ces acteurs, au travers de trois axes majeurs:
  - Transparence:
    - Délégué à la protection des données (DPD)
    - Registre des traitements
    - Documentation
  - Contrôle: obligation d'encadrer le personnel comme les sous-traitants
  - Sécurité:
    - Mesures préventives: systématisation de l'analyse de risque, prédominance de l'analyse d'impact
    - Mesures curatives: Notification et communication des violations de données

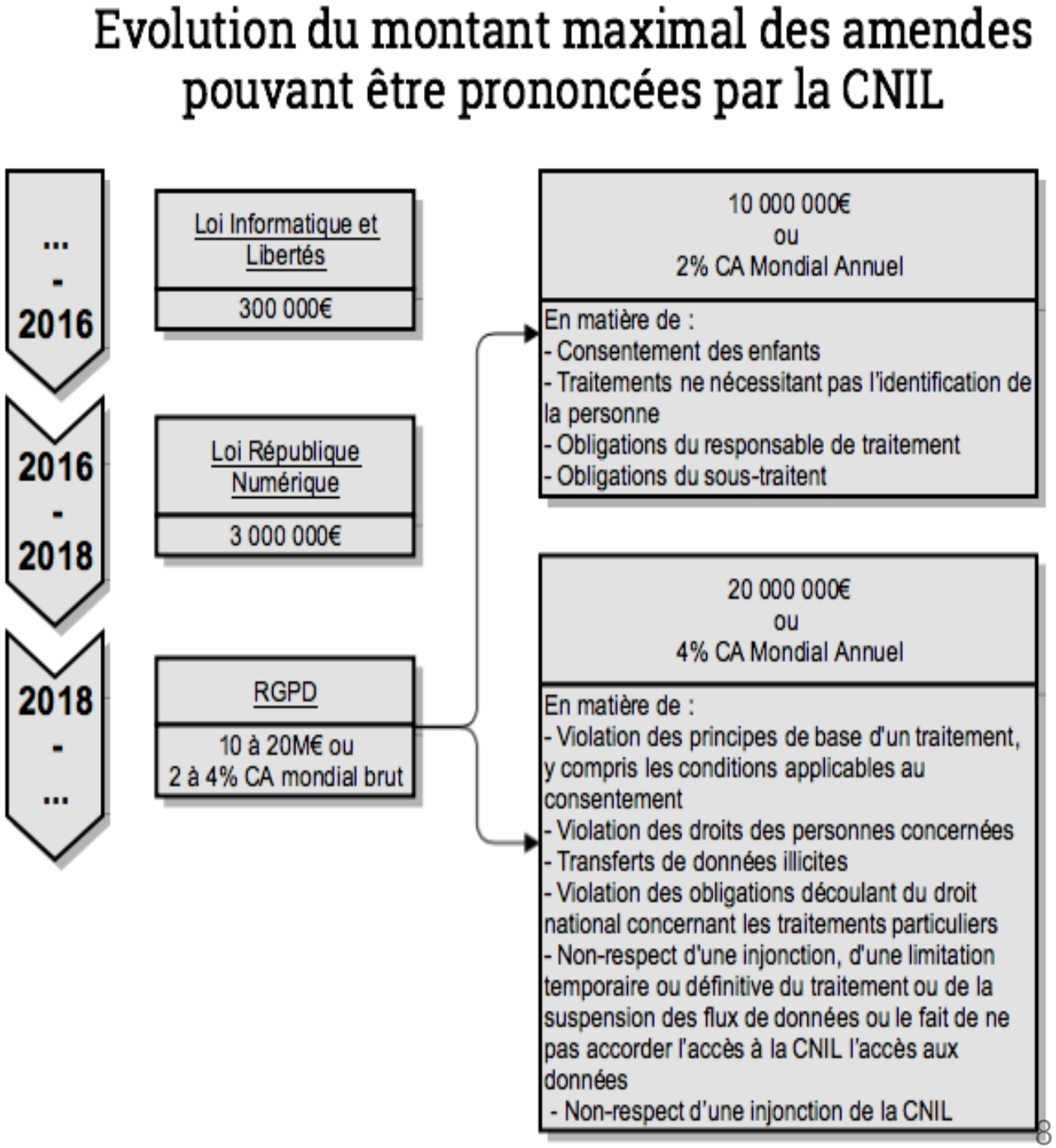
La fin de l'immunité du sous-traitant?

- Actuellement, un sous-traitant peut craindre un « *recours récursoire* » de son donneur d'ordre
- Avec le RGPD, il peut voir sa responsabilité engagée par la CNIL et encourt ainsi la même sanction que son donneur d'ordre



Sanctions et voies de recours

- Les sanctions prononcées par la CNIL pourront être contestées devant le Conseil d'Etat
- Le nombre de sanctions pourrait croître:
  - Obligation d'information quant à l'existence des recours
  - Création d'une action de groupe
  - Transfert probable des agents instructeurs aux *Contrôles*



La majorité de ces notions ne vous parle pas?

Le DPD, un RSSI juridique?

- Personne en charge du respect de la protection des données au sein de l'organisation
- Désignation recommandée, excepté notamment pour :
  - le traitement à grande échelle de données sensibles (dont santé) ➔ Hôpitaux directement visés
  - les organismes chargés d'une mission de service public ➔ Service Public Hospitalier
- Mutualisation possible, sous réserve que le DPD soit facilement joignable et ait une bonne connaissance des traitements ➔ Besoin d'harmoniser les traitements de données
- Rôle souvent assimilé au RSSI, mais pas nécessairement compatible

Le registre des traitements

- Obligatoire pour le responsable comme le sous-traitant, dès lors que le traitement porte sur des données de santé
- Contenu précisé dans le RGPD:
  - Informations relatives aux caractéristiques du traitement
  - Informations relatives aux modalités du traitement
  - Informations relatives aux acteurs du traitement
- La forme est libre (papier, Excel, logiciel ad hoc), du moment que les modifications peuvent être tracées
- Modèle sur le site de la CNIL
- Idéalement, y adjoindre un système de suivi des sous-traitants (identité, mission, date du contrat, date de fin, reconduction éventuelle)

L’analyse d’impact

- Processus consistant à étudier les conséquences sur la personne concernée d’une violation de données
- Obligatoire en cas de risques élevés:
  - Hôpitaux et ESMS ➔ risque toujours élevé car ils traitent des données sensibles relatives (potentiellement) à des personnes vulnérables, et ce à grande échelles
- Réalisée par le responsable de traitement avec l’aide du DPD (éventuellement mutualisé) et de ses sous-traitants, avant la mise en œuvre et préalablement à toute mise-à-jour
- Si l’analyse révèle un risque élevé si des mesures pour atténuer le risque n’étaient pas prises, consultation de la CNIL obligatoire
  - La demande doit comporter différentes informations et une copie de l’analyse

Documentation

- Obligation d'établir un dossier démontrant la conformité des traitements ou opération réalisées par le responsable et/ou son sous-traitant
- La documentation doit être tenue à disposition de la CNIL pour démontrer la conformité
  - Elle revient sur les caractéristiques juridiques, techniques et organisationnelles et modalités de traitement ainsi que sur la liste des participants
  - Elle argumente l'absence:
    - De désignation d'un Délégué à la Protection des Données
    - De réalisation d'une analyse d'impact
    - De mise en place d'un registre des traitements
  - Elle renvoie aux différentes politiques de l'organisation (PSSI, gestion des demandes des personnes concernées, etc.)

Conditions de recours à un sous-traitant

- Le sous-traitant doit présenter des garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles appropriées de manière à ce que le traitement :
  - réponde aux exigences du RGPD
  - garantisse la protection des droits de la personne concernée

- Contrat écrit sur support papier ou électronique
  - Plusieurs mentions obligatoires, dont :
    - Clause de confidentialité et clause d'audit
    - Clause d'encadrement de l'externalisation par le sous-traitant

- Intervention du sous-traitant sur instruction écrite et préalable

La sous-traitance, en pratique

1) Définir les procédures en interne et prévoir les conditions d'intervention des sous-traitants dans chacune

- Rôle dans la réponse aux demandes des personnes concernées
- Délai de notification d'une violation de données

2) Elaborer une clause de sous-traitance type pour l'entité

3) Revoir tous les contrats et soumettre un avenant RGPD

4) Etablir (et mener) un programme d'audit des sous-traitants

Une « convergence » entre le RGPD et la loi Touraine

RGPD

- Violations de données
- Notifiées à la CNIL
- Sous 72h

Loi Touraine

- Incidents graves de sécurité
- Déclarés à l'ARS
- Sans délai

La coresponsabilité, quel intérêt?

- Champ d'application non défini
  - Idéal pour le logiciel SAAS et les mutualisations (GCS, GHT?, etc.)
- Dans un monde idéal, quel intérêt?
  - Répartir clairement les responsabilités entre la ou les personnes déterminant la finalité et celles déterminant
  - Assurer une totale transparence vis-à-vis des personnes concernées et des autorités
- Dans le monde médical et médico-social, quel intérêt?
  - Rétablir l'équilibre avec des prestataires aux pratiques parfois abusives?

Avertissement

- En matière de traitement de données relatifs à la santé, les Etats membres de l'UE sont autorisés à maintenir ou introduire des conditions supplémentaires, y compris des limitations

DESMARAIS

AVOCATS

34, rue Pétrelle • 75009 PARIS
contact@desmarais-avocats.fr • www.desmarais-avocats.fr