Le RGPD en pratique pour les entreprises en santé : Les évolutions organisationnelles induites

Grenoble, Médic@lps – Janvier 2018

Maître Thomas ROCHE,
Avocat associé, DELSOL Avocats.
Responsable du département Sciences du vivant.
Avocat aux Barreaux de Lyon et Montréal.
troche@delsolavocats.com

DELSOL AVOCATS
LA QUALITÉ DE LA RELATION

Sommaire

- ✓ Introduction
  - Focus : les données de santé
- ✓ Le principe d'Accountability et ses conséquences pratiques
  - Focus : désignation d'un DPO
  - Focus : Réalisation d'une étude de risque préalable et d'une analyse d'impact
- ✓ Les pouvoirs des autorités de contrôle et les sanctions nouvelles
- ✓ En pratique : Constituer un registre des activités de traitement

Introduction

L'adoption du RGPD

Objectifs : remplacer la directive de 1995 et ainsi prendre en compte

- les évolutions technologiques des dernières années
- l'augmentation considérable de la collecte et des échanges de données personnelles
- les nouvelles modalités d'accès aux données

Renforcer les droits des citoyens sur leurs données personnelles

Prendre en compte l'intégration économique du fait du marché unique et **faciliter les flux de données**

Réduire les lourdeurs administratives et notamment les formalités préalables pesant sur les acteurs économiques

Assurer une **application homogène et cohérente** des règles de protection des données personnelles

Focus : les données de santé

Données de santé

Catégorie particulière de données : données sensibles

- ✓ Les données à caractère personnel concernant la santé devraient comprendre l'ensemble des données se rapportant à l'état de santé d'une personne concernée **qui révèlent des informations sur l'état de santé physique ou mentale passé, présent ou futur de la personne concernée**.
  - Informations sur la personne physique collectées lors de l'inscription de cette personne physique en vue de bénéficier de services de soins de santé ou lors de la prestation de ces services au bénéfice de cette personne physique
  - un numéro, un symbole ou un élément spécifique attribué à une personne physique pour l'identifier de manière unique à des fins de santé
  - des informations obtenues lors du test ou de l'examen d'une partie du corps ou d'une substance corporelle, y compris à partir de données génétiques et d'échantillons biologiques
  - et toute information concernant, par exemple, une maladie, un handicap, un risque de maladie, les antécédents médicaux, 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'un test de diagnostic in vitro.

Traitement de données de santé : interdiction de principe

- ✓ Exceptions :
  - le traitement est nécessaire **aux fins de la médecine préventive** ou de la médecine du travail, de l'appréciation de la capacité de travail du travailleur, **de diagnostics médicaux, de la prise en charge sanitaire ou sociale**, ou de la gestion des systèmes et des services de soins de santé ou de protection sociale sur la base du droit de l'Union, du droit d'un État membre ou en vertu d'un contrat conclu avec un professionnel de la santé et soumis aux conditions et garanties visées au paragraphe 3 (respect du secret professionnel);
  - 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;
- ✓ 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.

Le principe d'Accountability et ses conséquences pratiques

Les principes de protection des données (Art. 5)

- **Licéité, loyauté et transparence du traitement des données**
- **Limitation des finalités pour lesquelles les données sont collectées. Elles doivent être déterminées, explicites et légitimes.**
- **Minimisation des données collectées (adéquates, pertinentes et limitées à ce qui est nécessaire)**
- **Exactitude des données collectées**
- **Limitation de la conservation des données**
- **Intégrité et confidentialité du traitement**

Responsabilité : le responsable du traitement est responsable du respect de ces principes et doit être en mesure de le démontrer.

Suppression des formalités et consultations préalables

- Le règlement européen envisage la **suppression quasi-totale des formalités préalables** à accomplir auprès des autorités de contrôle, en particulier la CNIL.

- Le principe d'*accountability* se traduit par une **plus grande responsabilisation** des acteurs, notamment en supprimant les obligations déclaratives **dès lors que les traitements ne constituent pas un risque pour la vie privée des personnes**.

- Les fichiers pour lesquels des formalités ont déjà été régulièrement effectuées auprès de la CNIL (déclarations, autorisations accordées et avis rendus) pourront être poursuivis après le 25 mai 2018 sans devoir faire l'objet d'une éventuelle étude d'impact sur la vie privée tant qu'ils ne seront pas modifiés de façon substantielle.

- L'étude d'impact devant être régulièrement mise à jour, elle devra néanmoins être réalisée ultérieurement.

  - Ex : condamnation d'une pédiatre de l'AP-HM par le Tribunal de grande instance (TGI) de Marseille le 7 juin 2017 à 5.000 euros d'amende pour avoir mis en œuvre un traitement de données à caractère personnel sans autorisation de la CNIL.

Suppression des formalités et consultations préalables

Exceptions

- **Traitements présentant un risque élevé à l'issue de l'analyse d'impact et,**
- **pour lesquels le RT ne parvient pas à déterminer des mesures suffisantes pour atténuer ce risque.**

le RT communique à l'autorité de contrôle :

- les responsabilités respectives,
- les finalités et moyens du traitement,
- les mesures et les garanties prévues,
- les coordonnées du DPO,
- l'analyse d'impact,
- toute autre information.

- **Le droit des Etats membres (EM) peut prévoir l'obligation de consultation et d'autorisation préalable**

- **Traitements effectués dans le cadre d'une mission d'intérêt public, y compris protection sociale et santé publique. *(Article 36)***
- **Domaines réservés au droit national.**
  Ex : les ressources humaines ou la gestion du numéro d'identification national, les traitements à des fins archivistiques dans l'intérêt public, à des fins de recherches scientifique ou historique ou à des fins statistiques. *(Articles 85 à 91)*
- **Conditions supplémentaires pour le traitement des données génétiques, biométriques ou concernant la santé. *(Article 9)***
- **Contrôle de l'autorité public ou autorisation par le droit de l'Union ou par le droit de l'Etat membre pour les traitements des données relatives aux condamnations pénales et aux infractions (*Article 10)***

Les nouveaux outils du Privacy by design

❑ Privacy by design et privacy by default (Article 25)

Les responsables de traitement devront mettre en œuvre toutes les mesures techniques et organisationnelles nécessaires au respect de la protection des données personnelles, à la fois dès la conception du produit ou du service et par défaut.

- ***Privacy by design :*** les outils, produits, applications ou services intègrent de façon effective les principes relatifs à la protection des données. Ces principes s'appliquent :

- au moment de la détermination des moyens du traitement (ex: la pseudonymisation)

- pendant toute la durée de vie du traitement

- ***Privacy by default :*** les outils, produits, applications ou services garantissent que seules sont traitées les données nécessaires à la finalité du traitement au regard de la quantité de données collectées, de l'étendue de leur traitement, de la durée de conservation et du nombre de personne y ayant accès.

- Prévoir au minimum certaines protections : quantité de données traitées limitées et accessibilité restreinte, durée du traitement déterminée

Ex : prestataires de service ou concepteurs de logiciels peuvent prévoir que le paramétrage technique par défaut ne rende pas obligatoire le remplissage d'un champ facultatif.

La tenue du registre

Cette obligation **s'applique aux entreprises de plus de 250 personnes, sauf, pour les entreprises comptant moins d'effectifs, si le traitement présente un risque élevé, n'est pas occasionnel ou s'il comprend des catégories particulières de données. En pratique, la plupart des entreprises vont donc devoir tenir un registre.**

Obligation du CIL actuelle dans la Loi Informatique et Libertés	**Obligation du responsable de traitement, avec l'aide du DPO si nécessaire.** **Ajout de l'ensemble des transferts quel que soit leur fondement et des mesures de sécurité techniques et organisationnelles.**

➔ **Cette obligation s'applique aussi bien au responsable de traitement qu'au sous-traitant.**

La future loi Informatique et Libertés

- ✓ Chapitre IX – Traitements de données à caractère personnel dans le domaine de la santé
  - Section 1 - Dispositions générales
    - Exclusions des activités de diagnostic, prévention et soins
    - Traitement ne peuvent être mis en œuvre qu'en considération de la finalité d'intérêt public qu'ils présentent (quid de la vigilance, des entrepôts de données de santé, etc. ?)
    - CNIL en concertation avec INDS établit des référentiels et règlements types (ex: AU 13 – Traitement de pharmacovigilance, AU41 – ATU RTU, etc. ?)
    - RT doit adresser à la CNIL **une déclaration de conformité** (= étude d'impact + déclaration)
  - Section 2 - Dispositions particulières aux traitements à des fins de recherche, d'étude ou d'évaluation dans le domaine de la santé
    - Pas d'évolutions notables : Autorisation CNIL suivant avis CEREES ou CPP ou engagement /déclaration de conformité à une MR

Focus : désignation d’un DPO

La désignation du DPO est obligatoire dans trois cas

- Pour toute **autorité publique** ou tout **organisme public**.

Cela concerne notamment les collectivités territoriales, l'Etat, ou les établissements publics.
Le G29 recommande la désignation d'un DPO pour les organismes privés chargés d'une mission de service public

- Si **les activités de base de l'organisme** consistent en des traitements qui, du fait de leur nature, de leur portée et/ou de leurs finalités, exigent un **suivi régulier et systématique** à **grande échelle** des personnes concernées.

  Activités de base : cœur de métier, ou activités clés pour atteindre les objectifs de l'organisme (ex les Hôpitaux)
  Suivi régulier et systématique : récurrent et organisé
  Grande échelle : données clients d'une assurance ou d'une banque

- Si les activités de base de l'organisme consistent en des traitements à grande échelle de données sensibles, ou de données relatives aux condamnations et infractions spéciales.

  Ex : les hôpitaux, les applications web visant à échanger les données de santé, systèmes d'information médico-sociaux

❑ La désignation du DPO

Recommandations du G29 du 13 décembre 2016 et révisées le 5 avril 2017, relatives à la désignation du DPO.

- Le G29 recommande la désignation d'un DPO même hors des cas de désignation obligatoire. Il obéit aux mêmes règles.
- En cas d'absence de désignation, il est recommandé de documenter l'analyse menée pour déterminer la nécessité de désigner un DPO.
- Le DPO doit posséder des qualités professionnelles et une expertise dans le domaine des données personnelles.
- Le DPO est désigné pour l'ensemble des traitements mis en œuvre par l'organisme.

Qui désigner ?

➢ **Désigner un DPO externe ou interne**

- Le RGPD prévoit la possibilité de désigner un tiers pour exercer les missions de DPO via un contrat de prestation de service.

- Garantie d'indépendance du DPO telle qu'exigée par le règlement.

G29 : Il est recommandé de veiller à bien définir les missions du DPO par un contrat formalisant sa désignation. Particulièrement important pour la conduite de l'étude d'impact et la réalisation de missions en plus de ses obligations légales, comme la tenue du registre.

❑ Rôle et moyens (Article 38)

- Il doit être **associé, en temps utile**, **à toute question** relative à la protection des données.

  Privacy by design. Les process internes de l'entreprise doivent prévoir d'interroger le DPO et de l'associer aux prises de décisions impliquant le traitement de données.

- Il doit disposer des **ressources nécessaires à l'exécution de ses missions**.

  Ex : Il doit notamment pouvoir accéder aux traitements et services connexes et avoir été désigné officiellement afin de lui permettre d'assurer son rôle de contact.
  Il doit bénéficier d'une formation continue.

- Il doit **être indépendant** dans l'accomplissement de ses missions.

  Ex : Il ne reçoit pas d'instruction sur la manière d'exercer ses missions comme par exemple la nécessité de consulter l'autorité.

- Il n'encourt **pas de responsabilité et de sanctions** dans l'accomplissement de ses missions.

- Il **rapporte** directement au **degré le plus élevé de l'organisme**.

❑ Les missions du DPO (Article 39)

1. **Il informe et conseille** le responsable de traitement ou le sous-traitant.

2. **Il contrôle le respect des obligations** au titre du **RGPD** mais également des autres **législations des Etats membres** et des règles internes de l'organisme. Il participe également à la **formation du personnel**.

   Ex : le DPO pourra organiser des formations pour les salariés de l'entreprise et vérifier la conformité et l'application des politiques internes.
   G29 : les employés doivent être informés de sa nomination et de ses coordonnées.

3. **Il dispense des conseils concernant l'analyse d'impact et vérifie son exécution.**

   G29 : Son avis porte sur la nécessité ou non de réaliser l'étude d'impact, la méthode utilisée, les garanties à mettre en œuvre, l'exactitude du résultat et l'exécution de l'analyse d'impact. Le RT doit documenter toute décision contraire à l'avis du DPO.

4. **Il coopère avec l'autorité de contrôle**

   Ex : Il facilite l'accès aux documents et informations dans le cadre d'un contrôle ou d'une demande de précision de l'autorité.

5. **Il est le point de contact de l'autorité de contrôle concernant les questions relatives aux traitements, en particulier lorsque l'avis préalable de l'autorité est requis.**

❑ Les missions du DPO

Les missions du DPO ne sont pas limitatives. Il peut également intervenir :

➢ comme **point de contact des personnes concernées** par le traitement ;

Remarque : Ses coordonnées doivent être mentionnées parmi les informations obligatoires délivrées à la personne concernée.

➢ pour assurer la **bonne tenue du registre**.

Remarque : La tenue du registre incombe au RT ou au ST. Toutefois, cette mission peut être confiée au DPO qui pourra établir un bilan annuel des activités.

Focus : Réalisation d’une étude de risque préalable et l'analyse d’impact

L'étude de risques préalable et l'analyse d'impact (Art. 35)

L'analyse d'impact doit être effectuée par le responsable de traitement dès lors qu'un type de traitement, en particulier par le recours à de nouvelles technologies et compte tenue de la nature, de la portée, du contexte et de ses finalités, est ***susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques.***

Quand doit-on réaliser une analyse d'impact ?

Si le traitement remplit au moins deux des critères posés par le G29

1. Evaluation/Scoring
2. Décision automatique avec effet légal
3. Surveillance systématique
4. Données sensibles
5. Large échelle
6. Croisement de données
7. Personnes vulnérables
8. Usage innovant
9. Transfert hors UE
10. Blocage d'un droit/contrat

L'analyse d'impact n'est pas nécessaire

- Si le traitement n'est pas susceptible d'engendrer des risques élevés
- Si le traitement est déjà autorisé (tant qu'il respecte les conditions de mise en œuvre).
- Base légale

Attention : L'analyse d'impact doit être régulièrement renouvelée et mise à jour. Un traitement ayant fait l'objet d'une autorisation devra néanmoins faire l'objet d'une analyse d'impact ultérieurement.

Quelle méthode pour conduire l'analyse d'impact ?

1. Etude du contexte

Réalisation d'un schéma fonctionnel du traitement détaillant les flux de données personnelles et leurs supports, de leur collecte à leur destruction.

2. Etude des mesures

Identifier les mesures de sécurité juridique, physiques, logiques et organisationnelles mises en œuvre ou prévues par le responsable du traitement pour respecter les exigences légales et traiter les risques sur la vie privée de manière proportionnée.

3. Etude des risques

Identifier les violations potentielles des données, en précisant la gravité des impacts sur les personnes concernées et la vraisemblance des menaces rendant possibles ces violations.

4. Validation

Prendre la décision de valider la manière dont il est prévu de respecter les principes de protection de la vie privée et de traiter les risques, ou bien réviser les étapes précédentes.

Bâtir un dispositif de protection qui permette de traiter les risques de manière proportionnée et conforme aux principes du Règlement et qui tienne compte des contraintes du responsable du traitement.

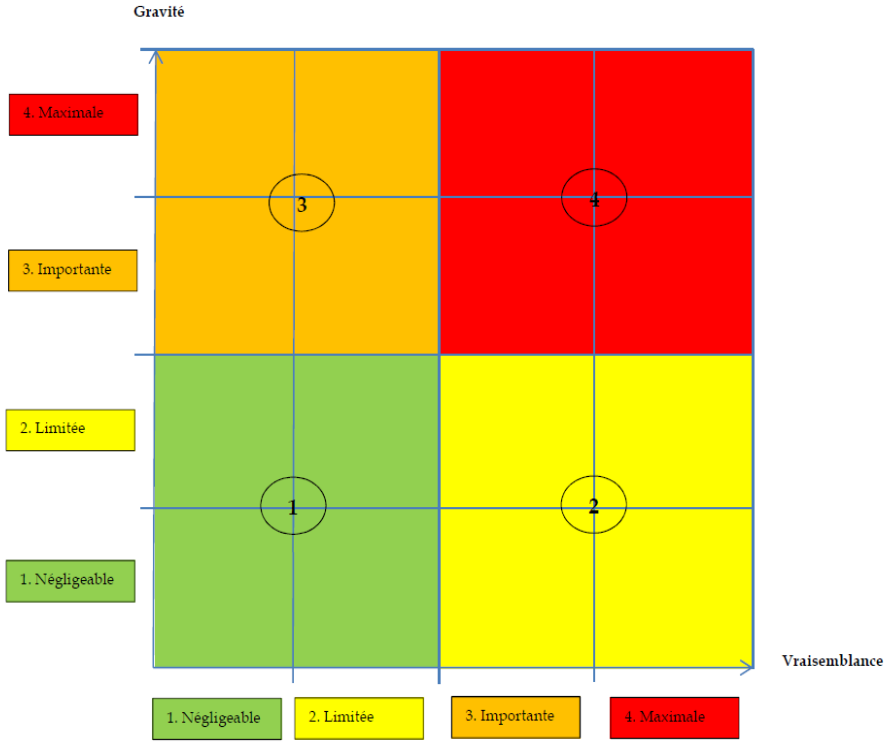
Focus : *Détermination de l'acceptabilité du risque :* utilisation de la méthode EBIOS

Zone n°4 : risques dont la gravité et la vraisemblance sont élevées :
Ces risques ne doivent pas être pris.

Zone n°3 : risques dont la gravité est élevée mais la vraisemblance faible :
Ces risques peuvent être pris, mais uniquement s'il est démontré qu'il n'est pas possible de réduire leur gravité et si leur vraisemblance est négligeable.

Zone n°2 : risques dont la gravité est faible mais la vraisemblance élevée :
Ces risques peuvent être pris, mais uniquement s'il est démontré qu'il n'est pas possible de réduire leur vraisemblance et si leur gravité est négligeable.

Zone n°1 : risques dont la gravité et la vraisemblance sont faibles :
Ces risques peuvent être pris.



Les pouvoirs des autorités de contrôle et les sanctions nouvelles

Les pouvoirs des autorités de contrôle étendus

Pouvoirs d'enquête

- Ordonner au RT, au ST ou leur représentant, la communication d'information
- Mener des enquêtes sous forme d'audit sur la protection des données
- Procéder à un examen des certifications
- Notifier au RT ou ST l'existence d'une violation des dispositions du RGPD
- Obtenir l'accès à toutes les DCP et informations nécessaires
- Obtenir l'accès à tous locaux ou installations et tout moyen de traitement

Des sanctions accrues

➢ **Sanctions dissuasives et proportionnelles de deux niveaux :**

Niveau 1 : Maximum 10 000 000 euros ou 2% du chiffre d'affaires mondial.

➢ **En particulier le non respect des obligations du responsable de traitement ou du sous-traitant dans l'organisation du traitement.**

Ex : absence de tenue d'un registre, le défaut de nomination d'un DPO ou absence de réalisation d'une étude d'impact

Niveau 2 : Maximum 20 000 000 euros ou 4% du chiffre d'affaires mondial.

➢ **Selon la nature du manquement aux règles de protection des données, en particulier le non respect des droits des personnes.**

Ex : le manquement au recueil du consentement de la personne concernée

➢ **Jusqu'à l'entrée en vigueur du règlement :**

- **Sanctions administratives :** Pouvoirs de la CNIL pouvant aller jusqu'à 3 millions d'euros.
- **Sanctions pénales** allant jusqu'à 300 000 euros et 5 ans d'emprisonnement pour une personne physique, et 1.5 millions d'euros pour une personne morale.

En pratique : Constituer un registre

Constituer son registre

Merci de votre attention !

Thomas ROCHE Avocat Associé
Avocat aux Barreaux de Lyon et Montréal

DELSOL Avocats
Avocats aux Barreaux de Lyon et Paris

11, quai André Lassagne - 69001 Lyon
Tél : 33 (0)4 72 10 20 30 - Fax : 33 (0)4 72 10 20 31

4 bis, rue du Colonel Moll - 75017 Paris
Tél : 33 (0)1 53 70 69 69 - Fax : 33 (0)1 53 70 69 60

Email : troche@delsolavocats.com
Site : www.delsolavocats.com
Blog: www.sciencesduvivant.delsolavocats.com

The information contained in this presentation has been given for an informative purpose only and cannot constitute a consulting neither a juridical advice.

Consequently it could never engage the responsibility of the author neither the responsibility of Delsol Avocats.

Any person wanting to use the information contained in this presentation will have necessarily to ask for professional advises from a person able to do so and specifically a professional competent in the juridical matters.

In accordance with the "Code de la propriété intellectuelle" anyone who would like to reproduce the content of this presentation, modified or not, in order to communicate directly or indirectly to the public (even if it is made for internal purpose) must imperatively request for a prior authorisation from Delsol Avocats.

Notwithstanding you will be authorised by Delsol Avocats to diffuse by any way the present document to the public only if you ensure to maintain the total integrity of the document. In particular you are forbidden to (i) suppress or modify any element of this document (ii) suppress the identity and function of the author(s), the name Delsol Avocats, the logos, the commercial brands, and more generally any distinctive element than can be connected to the authors or their companies.