Etats généraux du droit médical et du dommage corporel
Université Libre de Bruxelles
15 mai 2018

Le Règlement 2016/679 (GDPR) et les données de santé : questions choisies

Thierry Léonard
Avocat au barreau de Bruxelles
Professeur à l'Université Saint-Louis - Bruxelles
thierry.leonard@ulys.net

Bojana Salovic
Avocate au barreau de Bruxelles
bojana.salovic@ulys.net

www.ulys.net

Ulys - Cabinet d'avocats franco-belge, au service de la création et de l'innovation

PLAN

I. Introduction

II. Le régime particulier des données de santé

III. La transposition du GDPR en Belgique :

1) L'avant-projet de loi relatif à la protection des personnes physiques à l'égard des traitements de données à caractère personnel (« loi-cadre »)

2) L'avant-projet de loi instituant le comité de sécurité de l'information

I. Introduction

- De la Directive 1995/46 au Règlement 2016/679
- Evolution et modernisation des règles : protection accrue des personnes concernées et internet 2.0 + responsabilisation
- Entrée en application : 25 mai 2018

I. Introduction

- Problématique des lois d'implémentation
  - Marge de manœuvre importante laissée aux Etats même si Règlement européen;
  - Marge de manœuvre spécifique en matière de données de santé (art. 9.4 GDPR)

→ loi du 3 décembre 2017 sur l'autorité nationale de contrôle

→Deux avant-projets de loi… et ensuite?

II. Le régime particulier des données de santé

Le régime particulier des données sensibles

- Catégories particulières de données ou « données sensibles » :
  - Origine raciale ou ethnique, opinions politiques, convictions religieuses ou philosophiques, appartenance syndicale ;
  - Données génétiques et biométriques (nouveauté GDPR);
  - **Données de santé** ou vie/orientation sexuelle

Définition des données de santé

- Pas de définition dans le texte de la directive 95/46. Définition dégagée par la CJUE avec interprétation extensive (arrêt Linqvist)

- Définition explicite dans GDPR :

  « *les 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* »

- Exemples

Le principe et ses exceptions

- Principe : interdiction de traitement de données sensibles

- Exemple d'exceptions :
  - ✓Consentement explicite
  - ✓Sauvegarde intérêts vitaux
  - ✓Traitement par professionnel de la santé
  - ✓Archives intérêt public /recherche scientifique/statistiques

! Jamais l'exécution d'un contrat

Exception : le consentement explicite (Article 9.2.a) GDPR)

- Consentement comme base de licéité du traitement (article 7 GDPR)

Acte positif clair, libre, spécifique, éclairé et univoque

- Conséquences :

- implique possibilité de retrait du consentement (déjà prévu sous loi vie privée)

- consentement et conditions générales

Exception : le consentement explicite (Article 9.2.a) GDPR)

- Avant :
  - Directive 95/46 : « consentement explicite »
  - Loi vie privée : « consentement écrit »

- GDPR : Consentement explicite

(G29) : implique efforts supplémentaires

✓ Déclaration expresse et/ou écrite?

✓ Consentement en 2 étapes (double opt-in)

-> Position du G29 critiquable ?

Exception : intérêts vitaux (article 9.2.c) GDPR)

- Personne pas en mesure de manifester sa volonté : situation d'urgence médicale – question de vie ou de mort

- Que pour la dispensation de soins ! (pas la recherche médicale par ex)

Exception : professionnel de la santé (art. 9.2.h GDPR)

- Médecine préventive/du travail, diagnostics médicaux, prise en charge sanitaire/sociale, gestion de systèmes/services sanitaires/sociaux

+ garanties particulières : professionnel de la santé soumis à obligation de secret professionnel (article 9.3 GDPR)

Exception : professionnel de la santé (suite)

- Directive 95/46 : médecine préventive, diagnostics médicaux, administration de soins/traitements, gestion de services de santé

- Notion d'administration de soins/traitement pas couverte par GDPR : secteur médical OK mais autres, par exemple la délivrance de médicaments?

- Versions linguistiques divergentes : discrimination?

Exception : recherche scientifique (article 9.2.j) GDPR)

- Garanties article 89.1 GDPR : minimisation des données (pseudonymisation)

- Sur base du droit UE ou EM, proportionné, mesures appropriées pour sauvegarde droits fondamentaux et intérêts personne concernée

→titre IV de l'avant projet de loi (général) sur la protection des données

III. La transposition du GDPR en Belgique : la loi cadre et la loi instaurant CSI

1. Avant-projet de loi-cadre

- « Avant-projet de loi relatif à la protection des personnes physiques à l'égard des traitements de données à caractère personnel »

- Exécution de certains articles du GDPR ou marge de manœuvre laissée aux Etats membres

- Majorité du contenu : traitements du secteur public (transposition de la directive (UE) 2016/680; encadrement des flux issus d'autorités publiques, services de renseignement etc.)

1. Avant-projet de loi-cadre : structure

- **Titre 1 : De la protection des personnes physiques à l'égard du traitement des données à caractère personnel**
- Titre 2 : implémentation de la Directive 2016/680.
- Titre 3 : traitements d'autres autorités que celles visées aux titres 1 et 2.
- **Titre 4 : Traitement à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques**
- **Titre 5 : Voies de recours et représentation des personnes concernées**
- **Titre 6 : Sanctions**
- Titre 7 : L'organe de contrôle de l'information policière
- Titre 8 : dispositions finales (modificatives, abrogatoires…)

1. Avant-projet de loi-cadre : Titre 1

<u>De la protection des personnes physiques à l'égard du traitement des données à caractère personnel</u>

- Champ d'application territorial :
  - Etablissement du RT ou ST en Belgique
  - Personne concernée sur le territoire belge à qui on offre un service/bien sans établissement sur le territoire de l'UE

    -> Inspiration des critères du GDPR
- Avis 33/2018 CPVP : création de conflits de loi irrésolus et insécurité juridique (ex. : problème du ST établi en Belgique)

1. Avant-projet de loi-cadre : Titre 1

- Art. 9.4 du GDPR :

Etats membres ont la faculté d'introduire des conditions supplémentaires concernant traitements des données de santé

- Aucune mesure d'exécution prise dans l'avant-projet
  - Mais : Abrogation de l'AR 13.02.2001 et des garanties particulières prévues (art. 25 : peu appliquées…)
  - Avis 33/2018 CPVP : prévoir la réintégration de ces garanties dans l'avant-projet
  - Subsistance des dispositions prévues par législations particulières (AR 1999 dossier médical général, AR 2009 portant instructions pharmaciens,…)

1. Avant-projet de loi-cadre : Titre 1

- Traitement des données à caractère personnel relatives aux condamnations pénales et aux infractions (anc. données judiciaires) : exceptions limitées à l'interdiction de traitement

- Très nombreuses dérogations et limitations des droits de la personne en faveur du secteur public (principalement dans la recherche et le contrôle d'infractions, d'inspection ou de réglementation) :

1. Avant-projet de loi-cadre : Titre 1

- Encadrements des flux de données en provenance d'autorités/organismes publics fédéraux par un protocole d'accord (optionnel) entre responsables après avis des DPO

  → but : responsabilisation des autorités/organismes

  // principe de responsabilité/accountability du GDPR

  →Avis 33/2018 CPVP plutôt favorable

1. Avant-projet de loi-cadre : Titre 1

- Attention : tout sous-traitant d'une autorité publique/organisme public ou destinataire de données de ceux-ci devrait désigner un DPO!

1. Avant-projet de loi-cadre : Titre 4

<u>Traitements à des fins de recherche scientifique et statistiques</u>

- Champs élargi par rapport à l'AR de 2001 : tant pour les collectes directes que pour les traitements ultérieurs;
- Principe de base : anonymisation sauf si nécessaire de pseudonymiser ou nécessité de données « claires »;
- Régime distinct pour les collectes directes et les traitements ultérieurs qui sont favorisés

1. Avant-projet de loi-cadre : Titre 4

- Garanties générales pour tout traitement :

  -obligation de désignation d'un DPO

  - tenue d'un registre

  -documentation spécifique (not. sur le choix de données pseudonymisées ou non)

  -publicité du traitement…

- Avis 33/2018 CPVP sévère :
  - excessif et pas conforme au GDPR (approche par le risque)
  - Absence de prise en compte du contexte international de recherche

1. Avant-projet de loi-cadre : Titre 5

<u>Voies de recours et représentation des personnes concernées</u>

- Compétence du président du TPI (comme en référé) en cas de violation des règles protection données personnelles (introduit par la personne concernée ou l'APD ou organisation mandatée) + dommages et intérêts

- Avis 33/2018 CPVP :
  - Besoin de centraliser les procédures à Bruxelles (vu la spécialisation)
  - Lacune : devrait ouvrir l'action en cas de *risque* de violation grave

1. Avant-projet de loi-cadre : Titre 6

Sanctions

- Assouplissement des sanctions pour le secteur public
  - Pas de sanctions administratives (GDPR)
  - Sanctions pénales : 30.000€ max
- Cfr problème d'interprétation de ce qui relève du « secteur public »
- Avis 33/2018 CPVP : si pas d'amende, si pas d'interdiction du fait du principe de continuité, quelle sanction effective? La réponse pénale peine à convaincre…

2. Avant-projet de loi instituant le comité de sécurité de l'information

- Disparition de la CPVP, remplacée par l'APD

- CSQ : disparition des Comités Sectoriels.

- Tel le Phoenix : le Comité Sectoriel de la Sécurité Sociale et de la Santé + Comité Autorité Fédérale resurgissent…
  - Pouvoir de « délibération » (≠ autorisation mais serait contraignant à l'égard des tiers…)

2. Avant-projet de loi instituant le comité de sécurité de l'information

- Fin des procédures d'autorisations octroyées par Comité SS et Santé. Quid après 25 mai? Autorisations déléguées au CSI?

- Composition du CSI : chambre Sécurité Sociale et santé + chambre Autorité Fédérale

- Missions du CSI
  - Délibération concernant certaines communications de données;
  - Suivi des DPO des institutions de sécurité sociale et institutions publiques

2. Avant-projet de loi instituant le comité de sécurité de l'information

- Création d'un data warehouse dans la lutte contre la fraude sociale (datamatching et datamining)
  - Avis 34/2018 CPVP : contraire à l'article 8 CEDH, article 22 Constitution et au GDPR. Si exercice d'une mission d'intérêt public, alors dispositions spécifiques à respecter

- Limitation des droits des personnes en matière fiscale, fraude sociale, contrôles prévus par le CDE

2. Avant-projet de loi instituant le comité de sécurité de l'information

- Avis 34/2018 CPVP : favorable à la création d'un CSI mais défavorable quant à plusieurs points de l'avant projet
  - Composition du CSI et qualification des délibérations
  - Chèque en blanc pour « datawarehouse »
  - Incompatibilités avec le GDPR pour certaines limitations aux droits des personnes
  - Maintient de compétence d'autorisations pour certains flux de données contraire au principe de « délibérations »

Conclusions (très) provisoires

Sentiment de « malaise » prévaut :

- Trop et trop vite (!)…
- Pas de réflexion globale : régime des données de santé va rester plus que diffus et désordonné;
- Le CSI : implémentation juridique ou politique du GDPR?
- Un secteur public (trop) favorisé?

MERCI POUR VOTRE ATTENTION