Symposium VBS – GBS
3 février 2018
General Data Protection Regulation

Incidence du règlement général sur la protection des données sur la pratique médicale

Eric Thiry,
Avocat au barreau de Bruxelles

Se réjouir mais être préoccupé

Le nouveau règlement sur la protection des données (RGDP-GDPR) qui entre en vigueur le 25 mai 2018 fait l'objet de nombreux colloques et de multiples publications.

Le règlement en lui-même comprend 99 articles, plus de 150 considérants, soit près de 200 pages. Ce texte a fait l'objet de 4.000 amendements au cours de 4 ans de négociations.

Ce n'est toutefois pas une révolution juridique.

La plupart des principes étaient déjà applicables par le biais d'une directive européenne transposée dans la loi belge du 8 décembre 1992 relative à la protection des données à caractère personnel.

En tant que citoyen on peut donc se réjouir des efforts accrus pour protéger les données qui nous concernent.

Un des objectifs du règlement est d'établir « *des règles relatives à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et des règles relatives à la libre circulation de ces données* ».

En tant qu'acteur économique, il est temps de mettre fin à une certaine insouciance et de mesurer l'importance du respect de ce nouveau règlement : responsabilité et sanctions reviennent comme thèmes récurrents dans les colloques et commentaires.

Le M.B. du 10 janvier 2018 a publié la loi du 3 décembre 2017 portant création de l'Autorité de protection des données.

Cette Autorité succède à l'actuelle Commission de la protection de la vie privée et pourra notamment infliger des amendes administratives sans dépendre d'une autorisation du Parquet.

L'insouciance et les « justes » motifs de celle-ci

La règle fondamentale du respect du secret médical et les règles strictes du code de déontologie médicale ont entretenu la conviction de beaucoup de praticiens que, naturellement, ils respectaient la vie privée de leurs patients, ils ne conservaient que les données les concernant nécessaires à l'exercice de leur pratique et que dès lors ils étaient tous en règle avec les dispositions de la loi de 1992 sur la protection de la vie privée à l'égard des données personnelles…

AVIS DU 18 JANVIER 1997 DU CONSEIL NATIONAL DE L'ORDRE DES MÉDECINS SUR LES TRAITEMENTS AUTOMATISÉS DES DONNÉES À CARACTÈRE PERSONNEL

LOI DU 8 DÉCEMBRE 1992 RELATIVE À LA DÉCLARATION DE LA VIE PRIVÉE

DÉCLARATION DU FICHIER

« Tous les médecins qui tiennent des dossiers médicaux entrent dans le champ d'application de cette loi, qu'ils procèdent au moyen de fichiers manuels ou au moyen de traitements automatisés ».

Il appartient à chaque médecin de déclarer auprès de la Commission de la protection de la vie privée, les traitements automatisés déjà en cours et dorénavant également avant la mise en œuvre d'un traitement automatisé.

L'Ordre rappelle que la Commission de la protection de la vie privée a élaboré un formulaire destiné à la déclaration d'un traitement automatisé, formulaire qui comporte deux parties, une relative à l'identification du maître du fichier qui fait la déclaration et l'autre qui porte sur la description du traitement automatisé qui fait l'objet de la déclaration.

Dans le but de faciliter les déclarations pour une partie du corps médical, le Conseil national de l'Ordre avait préparé 4 déclarations standards susceptibles de rencontrer les buts du traitement et les catégories de données traitées pour :

- Le médecin travaillant comme indépendant dans son cabinet médical,
- La société professionnelle unipersonnelle d'un médecin,
- La société professionnelle de plusieurs médecins,
- Le médecin travaillant au sein d'une association de médecins sans personnalité juridique.

L’avis rappelle que ces déclarations standards ne concernent que les médecins qui traitent des données à caractère personnel, à titre individuel, par opposition à ceux qui, par exemple, au sein d’une institution de soins, participent à l’élaboration d’un dossier dont l’institution est le maître du fichier.

Les déclarations de fichiers médicaux informatisés devaient être faites avant la fin du mois de mai 1997.

Le Conseil national avait également préparé le texte d’une affichette à apposer au niveau de la salle d’attente ou du cabinet et destinée à informer de ses droits le public dont les données personnelles seront traitées.

Principales obligations s'adressant aux maîtres de fichiers manuels et aux maîtres de fichiers automatisés (rappelées dans l'avis de l'Ordre).

Si les données sont recueillies directement auprès de la personne concernée, elle doit être informée de l'identité et de l'adresse du maître du fichier, de la base légale réglementaire de la collecte des données, de la finalité pour laquelle les données recueillies sont utilisées, de la possibilité d'obtenir des renseignements complémentaires auprès du Registre public des traitements automatisés que crée la Commission de la protection de la vie privée, le droit d'accéder aux données ainsi que le droit de demander la rectification de celles-ci.

L'Ordre donnait un exemple de projet d'affiche qui rappelait que la loi de 1992 s'applique au traitement des données personnelles recueillies auprès des patients par le médecin et les données étaient traitées et conservées sous le contrôle et la responsabilité du médecin et l'existence du fichier automatisé est mentionnée dans le Registre public des fichiers de données personnelles informatisées et tenues auprès de la Commission de la protection de la vie privée … etc.

L'avis mentionne aussi que le Conseil national de l'Ordre avait élaboré des déclarations standards pour 4 types de buts puisqu'une déclaration séparée est requise par but de traitement automatisé.

Ces buts sont :

- Soins des patients, c'est-à-dire le diagnostic et le traitement paramédical des patients;
- Administration des patients, c'est-à-dire le suivi du séjour et du traitement des patients en vue de la facturation;
- Enregistrement de groupes à risques, c'est-à-dire l'identification et le suivi de personnes présentant un risque médical;
- Autres buts : constitution d'un fichier patients sur base de diagnostics.

Dans ces déclarations standards, les données relatives à la description du traitement à déclarer (partie 2 de la déclaration) sont déjà remplies et le médecin qui recourt à la déclaration standard ne doit plus remplir que la première partie de la déclaration (données d'identification concernant le maître du fichier).

Enfin l'avis rappelle que le fait de se référer à une déclaration standard n'exonère aucunement le maître du fichier de sa responsabilité concernant le caractère exact et complet de sa déclaration.

Bref, la Commission de la protection de la vie privée comme l'Ordre national des médecins ont fourni des « outils » pour permettre au médecin de se mettre en conformité avec la loi de 1992.

* *

*

Protection renforcée voulue par le RGPD

Cons.(11)«*Une protection effective des données à caractère personnel dans l'ensemble de l'Union exige de renforcer et de préciser les droits des personnes concernées et les obligations de ceux qui effectuent et déterminent le traitement des données à caractère personnel, ainsi que de prévoir, dans les Etats membres, des pouvoirs équivalents de surveillance et de contrôle du respect des règles relatives à la protection des données à caractère personnel et des sanctions équivalentes pour les violations* ».

Définitions rappelées à l'article 4 du RGPD

Données à caractère personnel :

Toute information se rapportant à une personne physique identifiée ou identifiable et réputée être une personne physique identifiable ou une personne physique qui peut être identifiée directement ou indirectement, notamment par la référence à un identifiant tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale.

Traitement :

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.

Pseudonymisation :

Le traitement de données à caractère personnel de telle façon que celles-ci ne puissent plus être attribuées à une personne concernée précise sans avoir recours à des informations supplémentaires, pour autant que ces informations supplémentaires soient conservées séparément et soumises à des mesures techniques et organisationnelles afin de garantir que les données à caractère personnel ne sont pas attribuées à une personne physique identifiée ou identifiable.

Fichier :

Tout ensemble structuré de données à caractère personnel accessible selon des critères déterminés, que cet ensemble soit centralisé, décentralisé ou réparti de manière fonctionnelle ou géographique.

Responsable du traitement :

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

Consentement de la personne concernée :

Toute manifestation de volonté, libre, spécifique, éclairée et univoque par laquelle la personne concernée accepte, par une déclaration ou par un acte positif clair, que des données à caractère personnel la concernant fassent l'objet d'un traitement.

Violation de données à caractère personnel :

Une violation de la sécurité entrainant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non-autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou l'accès non autorisé à de telles données.

Données génétiques :

Les 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.

Données biométriques :

Les données à caractère personnel résultant d'un traitement technique spécifique, relatives aux caractéristiques physiques, physiologiques ou comportementales d'une personne physique qui permettent ou confirment son identification unique, telles que des images faciales ou des données dactyloscopiques.

Données concernant la santé :

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 révèle les informations sur l'état de santé de cette personne…

Prise de conscience des obligations du responsable du traitement

Le RGPD identifie 10 principes directeurs :

Licéité, loyauté, transparence, limitation des finalités, minimisation des données, exactitude, limitation de la conservation, intégrité, confidentialité et responsabilité.

Dans le respect de ces principes, le responsable du traitement doit mettre en œuvre des mesures techniques et organisationnelles appropriées pour s'assurer être en mesure de démontrer que le traitement est effectué conformément au RGPD.

Ces mesures doivent être adoptées dès le début des activités de traitement.

La Commission de la protection de la vie privée a mis en ligne un document utile : « *Préparez-vous en 13 étapes* »

Les nouvelles obligations applicables au consentement

Cons. (32) « Le consentement devrait être donné par un acte positif clair par lequel la personne concernée manifeste de façon libre, spécifique, éclairée et univoque son accord au traitement des données à caractère personnel la concernant, par exemple au moyen d'une déclaration écrite, y compris par voie électronique, ou d'une déclaration orale.

Cela pourrait se faire notamment en cochant une case lors de la consultation d'un site internet, en optant pour certains paramètres techniques pour le service de la société de l'information ou au moyen d'une autre déclaration ou d'un autre comportement indiquant clairement dans ce contexte que la personne concernée accepte le traitement proposé de ses données à caractère personnel.

Il ne saurait dès lors y avoir de consentement en cas de silence, de cases cochées par défaut ou d'inactivité. Le consentement donné devrait valoir pour toutes les activités de traitement ayant la ou les mêmes finalités…

Si le consentement de la personne concernée est donné à la suite d'une demande introduite par voie électronique, cette demande doit être claire et concise et ne doit pas inutilement perturber l'utilisation du service pour lequel il est accordé ».

RGPD Article 7.1.« *Dans le cas où le traitement repose sur le consentement le responsable du traitement est en mesure de démontrer que la personne concernée a donné son consentement au traitement de données à caractère personnel la concernant.*

…

La personne concernée a le droit de retirer son consentement à tout moment. Le retrait du consentement ne compromet pas la licéité du traitement fondé sur le consentement effectué avant ce traitement.

La personne concernée en est informée avant de donner son consentement.

Il est aussi simple de retirer que de donner son consentement.

… »

Etendue des droits des personnes concernées (patients)

Le RGPD précise un grand nombre de droits pour les personnes concernées par le traitement des données.

- Droit d'accès aux données à caractère personnel traitées (art. 15);
- Droit de rectification (art. 16);
- Droit à l'effacement (droit à l'oubli) (art. 17);
- Droit à la limitation du traitement (art. 18);
- Droit à la portabilité des données (art. 20);
- Droit d'opposition et prise de décision individuelle automatisée (art. 21 et 22).

Nouveau principe de responsabilité

Le responsable du traitement doit mettre en œuvre des mesures techniques et organisationnelles appropriées pour s'assurer être en mesure de démontrer la conformité avec le RGPD (article 24).

La note d'information de la Commission de la protection de la vie privée prévoit comme deuxième étape le registre des données et précise:

« *Faites l'inventaire des données à caractère personnel que vous conservez, notez quelle est leur origine et les personnes avec lesquelles vous les avez partagées. Enregistrez vos traitements. Vous devez éventuellement organiser un audit d'information à cet effet* ».

Le registre des activités de traitement (article 30)

Le responsable du traitement tient un registre des activités de traitement effectuées sous sa responsabilité. Le registre comprend notamment comme informations :

- Le nom et les coordonnées du responsable du traitement;
- Les finalités du traitement ;
- Une description des catégories des personnes concernées et des catégories des données à caractère personnel ;
- Les catégories de destinataires auxquels les données à caractère personnel ont été ou seront communiquées;
- Dans la mesure du possible les délais prévus pour l'effacement des différentes catégories des données ;
- Dans la mesure du possible une description générale des mesures de sécurité techniques et organisationnelles

Si l’article 30 §5 prévoit que ces obligations ne s’appliquent pas à une entreprise ou à une organisation comptant moins de 250 employés, elles s’imposent dans le cadre de traitement de données relatives à la santé notamment (article 9 §1).

Le délégué à la protection des données

Une des nouveautés du RGPD consiste dans la désignation du délégué à la protection des données par le responsable du traitement, notamment lorsque :

Les activités de base du responsable du traitement (ou du sous-traitant) consistent en un traitement à grande échelle de catégories particulières de données (notamment les données relatives à la santé : article 37 §1, c renvoyant à l'article 9 du règlement).

La notion de « grande échelle » paraît assez floue.

Sans doute les médecins extra hospitaliers, travaillant en cabinet privé ou en petite structure ne sont-ils pas visés par cette notion de « grande échelle ».

Quid de ceux qui travaillent dans des centres médicaux ou des polycliniques intégrées ?

La prudence commandera sans doute de désigner un délégué à la protection des données et d'informer l'autorité de protection des données (ancienne Commission de la protection de la vie privée) de son identité.

Mission du délégué à la protection des données

Informer et conseiller sur le RGPD et les lois nationales,
contrôler le respect du RGPD,
former le personnel...

Obligations en cas de violation des données à caractère personnel

L'article 4,12 définit la violation des données à caractère personnel comme étant une violation de la sécurité entraînant, de manière accidentelle ou illicite la destruction, la perte, l'altération, la divulgation non autorisée des données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou l'accès non autorisé à des telles données.

En cas de violation, le responsable du traitement notifie cette violation à l'autorité de contrôle dans les meilleurs délais et, si possible, 72h au plus tard après en avoir pris connaissance, à moins que la violation ne soit pas susceptible d'engendrer un risque pour les droits et libertés des personnes physiques.

Si la notification n'a pas lieu dans les 72h. elle est accompagnée du motif du retard (article 33 §1).

Si la violation des données à caractère personnel est susceptible d'engendrer un risque élevé pour les droits et libertés d'une personne physique, le responsable du traitement communique aussi cette violation des données à la personne concernée dans les meilleurs délais.

Les missions de l'Autorité de contrôle

L'Autorité de protection des données (loi du 3 décembre 2017) est composée de 6 organes :

- 1 comité de direction
- 1 secrétariat général
- 1 service de première ligne
- 1 centre de connaissance
- 1 service d'inspection
- 1 chambre contentieuse

Le service de première ligne reçoit les plaintes et demandes. Il peut lancer une procédure de médiation. Il promeut la protection des données auprès du public. Il promeut auprès des responsables de traitement et des sous-traitants la prise de conscience de leurs obligations. Il fournit des informations relatives à l'exercice de leurs droits aux personnes concernées (article 22 - Loi du 3 décembre 2017).

Le centre de connaissance émet des avis et des recommandations.

Le service d'inspection est l'organe d'enquête de l'Autorité de protection des données.

La chambre contentieuse est l'organe contentieux administratif de l'Autorité de protection des données.

Enfin, il y a un conseil de réflexion qui émet des avis non contraignants à l'attention de l'Autorité de protection des données.

Les services d'inspection de l'Autorité de protection des données ont notamment le pouvoir de mener un examen sur place.

L'article 78 de la loi du 3 décembre 2017 prévoit :

« Lorsque l'inspecteur général et les inspecteurs ont des raisons de penser qu'une infraction aux principes fondamentaux de la protection des données à caractère personnel, dans la cadre de la présente loi et des lois contenant des dispositions relatives à la protection du traitement des données à caractère personnel est commise, ils peuvent pénétrer à tout moment dans l'entreprise, le service, ou tout autre endroit pour procéder à un examen sur place afin d'y faire des constatations matérielles.

Sauf accord écrit de la personne concernée ou autorisation du juge d'instruction, l'inspecteur général et les inspecteurs ne peuvent, sans la présence d'un représentant de l'ordre professionnel, pénétrer dans les locaux d'un professionnel qui est soumis au secret professionnel et pour qui une règlementation légale est prévue concernant l'examen sur place et l'accès à leurs locaux professionnels».

Le RGPD (article 57) énumère les missions de l'Autorité de contrôle. On retiendra en particulier :

Art. 57,1d. Encourager la sensibilisation des responsables du traitement et des sous-traitants en ce qui concerne les obligations qui leur incombent en vertu du présent règlement

1e. Fournir sur demande à toute personne concernée des informations sur l'exercice des droits que lui confère le présent règlement.

1f. Traiter les réclamations introduites par une personne concernée

1h. Effectuer des enquêtes sur l'application du présent règlement ... etc.

Droit à réparation et responsabilité (article 82)

Toute personne ayant subi un dommage matériel ou moral du fait d'une violation du règlement a le droit d'obtenir du responsable du traitement ou du sous-traitant réparation du préjudicie subi.

Tout responsable du traitement ayant participé au traitement est responsable du dommage causé par le traitement qui constitue une violation du règlement.

Possibilité d'être exonéré de responsabilité en apportant la preuve de l'absence de lien de causalité.

S'il y a plusieurs responsables du dommage, celui qui a indemnisé dispose d'un recours contre les co-responsables.

Les amendes administratives

L'article 83 du règlement prévoit les conditions générales pour imposer des amendes administratives et les montants peuvent être fort élevés.

Prise en compte des facteurs suivants :

- La nature, la gravité, la durée de l'infraction;
- Les catégories de personnes concernées qui ont été affectées;
- Le caractère intentionnel ou non de l'infraction;
- Les mesures qui ont été prises pour atténuer les dommages subis par les personnes concernées;
- La récidive éventuelle;
- La coopération avec les autorités de contrôle.

Sanctions

Selon l'article 84 du règlement les Etats membres déterminent le régime des autres sanctions applicables, en particulier pour les violations qui ne font pas l'objet des amendes administratives et ils prennent toutes les mesures nécessaires pour garantir leur mise en œuvre.

La loi du 3 décembre 2017 portant création de l'Autorité de protection des données a prévu que la chambre contentieuse a notamment comme pouvoir :

- Prononcer la suspension du prononcé
- Proposer une transaction;
- Formuler des avertissements et des réprimandes;
- Ordonner de se conformer aux demandes de la personne concernée d'exercer ses droits;
- Ordonner que l'intéressé soit informé du projet de sécurité;
- Donner des astreintes;
- Transmettre le dossier au Parquet du Procureur du Roi de Bruxelles qui l'informe des suites données au dossier;
- Décider au cas par cas de publier ses décisions sur le site Internet de l'Autorité de protection des données…(Article 100)

Collaboration au niveau national

L'article 52 §1er de la loi du 3 décembre 2017 prévoit que :

« *L'Autorité de protection des données accomplit ses missions dans un esprit de dialogue et de concertation avec tous les acteurs publics et privés concernés par la politique de la protection des libertés et des droits fondamentaux des personnes physiques à l'égard du traitement et du libre flux des données à caractère personnel ainsi que par la politique de la protection des consommateurs.*

L'Autorité de protection des données peut être assistée par ou agir à la demande d'autres pouvoirs publics chargés du respect d'autres législations ».

Conclusion

De gros efforts sont faits depuis de nombreux mois par les autorités publiques et de nombreuses organisations privées, professionnelles, syndicales et autres pour informer les entreprises, les acteurs économiques en général, les professions libérales en particulier, de l'entrée en vigueur du RGPD le 25 mai 2018,

Une collaboration efficace et constructive paraît nécessaire entre la nouvelle Autorité de protection des données et les Ordres, comme l'Ordre des médecins et les organisations professionnels pour la sensibilisation des responsables de traitement de données à leurs obligations et pour leur faciliter la tâche dans le respect de celles-ci.

Conseiller, accompagner, renseigner paraissent être les missions primordiales à remplir dans la première période d'entrée en vigueur de la loi.

Les enquêtes et les sanctions devraient être réservées à ceux qui seraient malgré tout restés encore coupables d'insouciance.

MERCI POUR VOTRE ATTENTION