Fiche 3.

La pratique de groupe

Check-list des bonnes pratiques à respecter :

→ J'identifie quelle est ma responsabilité au regard du RGPD ;

→ Si je suis responsable conjointement avec un ou plusieurs autres prestataires de soins, je veille à formaliser nos relations dans une convention précisant les règles de réparation des obligations du RGPD ;

→ Quel que soit le régime de responsabilité sous lequel j'exerce mes activités de soins :

Je respecte les grands principes de protection des données ;

Je m'engage à informer mes patients et m'assure du respect de leurs droits ;

Je veille à répondre aux obligations instituées par le RGPD (registre des traitements, mesures de sécurité, contrats de sous-traitance, notification des fuites de donnée à l'Autorité de Protection des Données (ADP)).

C'est un fait maintenant établi : les professionnels de la santé tendent à délaisser leurs cabinets individuels pour exercer en groupe sous la forme d'un **cabinet monodisciplinaire** ou d'un **cabinet multidisciplinaire de première ligne** (ex : une maison médicale).

Dès lors que **la continuité des soins est assurée en groupe**, il importe d'identifier, parmi les différents acteurs impliqués dans le traitement des données à caractère personnel, celui ou ceux qui seront considérés comme **responsables de traitement au sens du RGPD**.

La notion de responsable du traitement et son interaction avec la notion de responsable conjoint jouent un rôle central pour **déterminer la ou les personnes investies de la mission d'assurer le respect des règles de protection des données et, notamment, la manière dont les personnes concernées vont pouvoir exercer leurs droits.**

Qui est responsable de traitement au sens du RGPD ?

1. Définition

Le RGPD définit le responsable du traitement comme « *la personne physique ou morale, une autorité publique, une agence ou un autre organisme qui, **seul ou conjointement avec d'autres**, **détermine les finalités et les moyens** du traitement des données à caractère personnel* »[1].

Le critère principal permettant de considérer une personne comme responsable de traitement au sens du RGPD repose dans **la détermination des finalités et des moyens** de l'activité de traitement des données personnelles.

Le responsable du traitement est donc celui qui dans les faits (peu importe la répartition des rôles dans une convention) décide :

- du **quoi** : quelles données sont traitées ?
- du **pourquoi** : à quelles fins les données sont utilisées ?
- du **comment** : quels sont les moyens qui sont mis en œuvre ?

Identifier le responsable du traitement des données revient à identifier *in concreto* celui qui prend les **décisions** concernant le traitement des données (les types de données traitées, qui peut accéder à quelles données, s'il est fait appel à un sous-traitant externe, le délai de conservation des données, les systèmes techniques utilisés, etc.).

La responsabilité d'un traitement de données peut aussi reposer sur une ou plusieurs personnes (« *seul ou conjointement* »). Si les finalités et les moyens du traitement sont déterminés par plusieurs entités juridiques distinctes, celles-ci seront alors considérées comme **responsables conjoints** du traitement qu'elles mettent en œuvre[2].

[1] Article 4, 7° du RGPD.
[2] Article 26 du RGPD.

Il n'est cependant pas exigé que l'influence des responsables conjoints soit identique ou qu'ils puissent satisfaire individuellement aux obligations du RGPD. L'élément déterminant réside dans le fait qu'**ils disposent chacun d'une compétence décisionnelle**, dans une mesure identique ou non, et même si leur accès aux données personnelles est différent.

2. Règle d'or

En ce qui concerne la pratique de groupe, **la règle d'or** veut que **l'entité juridique** puisse être considérée comme **responsable de traitement** pour toutes les activités de traitement qu'elle organise sous son égide. En prenant l'initiative d'organiser certaines activités médicales, de soins et de support, l'entité juridique exercera une influence sur la manière dont les finalités et les objectifs de traitement des données seront atteints.

Par conséquent, si vous exercerez votre activité de soins au sein d'un cabinet monodisciplinaire (*ex : un cabinet de kinésithérapeutes ou un cabinet de médecine générale*) ou d'un cabinet multidisciplinaire (*ex : une maison médicale ou une polyclinique*), c'est l'entité juridique sous laquelle vous exercez votre activité de soins qui sera considérée comme responsable de traitement au sens du RGPD. Il lui appartient donc de se mettre en conformité avec les exigences relatives à la protection des données.

3. Groupement ayant la personnalité juridique

Si la règle d'or veut que ce soit l'entité juridique qui soit considérée comme responsable de traitement, deux hypothèses doivent être distinguées :

➢ Les moyens alloués à la tenue de vos dossiers patients sont définis par l'entité juridique sous laquelle vous exercez votre mission de soins

En définissant les moyens alloués à la tenue des dossiers patients, l'entité juridique sous laquelle vous exercez votre activité de soins est considérée comme responsable de traitement au sens du RGPD et veillera à la mise en œuvre des exigences et obligations du RGPD. Si vous êtes bien indépendant dans l'exercice de l'art de guérir, pour lequel vous ne recevez aucune instruction de la part de l'entité sous laquelle vous exercez votre activité, vous ne disposez pas d'une compétence décisionnelle dans les outils d'information mis à votre disposition. En exploitant le « logiciel métier » (« dossier patient ») mis à votre disposition par le cabinet de soins, vous agissez en tant que « **collaborateur** »[3], au même titre que tout autre employé du cabinet de soins, **quel que soit votre statut social (indépendant ou salarié) et quelle que soit la forme du contrat de collaboration qui vous lie au cabinet de soins.** Il vous appartient alors de vous conformer aux directives relatives à l'utilisation des outils d'information mis à votre disposition et au code de bonne conduite rédigé et publié par cette dernière.

[3] Le terme « collaborateur » est utilisé pour désigner toute personne travaillant à et/ou pour l'entité juridique, quel que soit son statut (indépendant ou salarié) et quelle que soit la forme du contrat de collaboration qui le lie à l'entité juridique, c'est-à-dire toute personne qui utilise les outils d'information définis par l'entité juridique pour s'acquitter de ses tâches.

- Les moyens alloués à la tenue de vos dossiers patients sont définis par vous-mêmes, c'est-à-dire que vous disposez de votre propre dossier patient pour l'exercice de votre activité professionnelle

Si vous tenez vos dossiers patients via un système qui vous est propre, c'est-à-dire en toute autonomie vis-à-vis de l'entité juridique sous laquelle vous exercez votre mission de soins (vous avez votre propre « logiciel métier »), vous êtes considéré comme **responsable de traitement au sens du RGPD.** Même si vous exercez votre activité professionnelle sous la même entité juridique que vos collaborateurs, vous ne partagez pas nécessairement avec eux les mêmes « finalités » et « moyens » de traitement des données de vos patients. L'entité juridique sous laquelle vous exercez ne pourra donc pas intervenir en qualité de responsable de traitement, car elle n'exerce aucune influence déterminante sur la définition des finalités et des moyens de traitements que vous effectuez.

4. Association de fait

Lorsque vous faites un groupement sous la forme d'une association de fait, notamment en vue de faire l'acquisition de ressources communes (locaux, secrétariat, équipements médicaux et bureautiques), la même distinction doit être faite :

- **Si vous exercez votre activité professionnelle avec des outils d'informations qui vous sont propres** (vous avez vos propres dossiers patients), vous êtes considéré comme **responsable de traitement au sens du RGPD** et à ce titre, vous êtes tenus de vous conformer au RGPD.

- En revanche, si, dans le cadre de votre activité professionnelle, **vous tenez vos dossiers patients de manière conjointe avec vos collaborateurs** (vous disposez d'un logiciel métier « commun » avec votre/vos collaborateurs), c'est-à-dire que vous partagez les mêmes finalités et moyens de traitement des données de vos patients, vous êtes considérés comme **responsables conjoints**. Vous devez donc veillez ensemble à la mise en œuvre des exigences et obligations du RGPD en tenant compte des spécificités liées au régime de la responsabilité conjointe (*voir ci-dessous*).

5. Pratique de « groupe » et pratique « solo »

Dans l'hypothèse où vous exercez votre activité professionnelle en partie au sein d'une entité mono ou pluridisciplinaire et en partie dans un cabinet « privé », vous devez distinguer vos activités au sein du cabinet mono ou pluridisciplinaire sous lequel vous exercez votre activité professionnelle et pour lequel vous pouvez être considéré comme un « collaborateur » et vos activités « privées ».

Au sein de votre cabinet privé, vous serez toujours considéré comme responsable de traitement à part entière. L'entité juridique sous laquelle vous exercez une partie de vos activités de soins n'intervient dans la gestion des données des patients que vous voyez en « privé ».

Si vous exercez votre activité professionnelle en partie dans une maison médicale par exemple, en tant que responsable de traitement (et non comme un « collaborateur ») et en partie dans un cabinet privé tout en allouant les mêmes finalités et moyens au traitement des données de vos patients (vous utilisez le même « logiciel métier » à votre cabinet privé qu'au sein du cabinet de soins auquel vous êtes associé), **vous ne devez pas vous conformer « doublement » aux exigences et obligations du RGPD** ! En effet, même si les lieux de vos consultations différent, les garanties de protection que vous accordez aux données de vos patients restent elles identiques.

Quelles sont vos obligations respectives ?

Une fois identifié, le responsable du traitement des données et son éventuel responsable conjoint devront se conformer à une série d'obligations dont l'intensité sera liée aux caractéristiques du régime de responsabilité dans lequel s'inscrit leur activité professionnelle.

1. Respecter les grands principes du RGPD

Chaque responsable de traitement est tenu de respecter les principes directeurs du RGPD[4]:

- ✓ **Licéité, loyauté et transparence :** Vous devez vous assurer que le traitement des données est légitime et que vous ne cachez rien aux personnes concernées. Restez transparents avec ces dernières en indiquant dans votre politique de confidentialité le type de données collectées ainsi que les raisons pour lesquelles vous les collectez.

- ✓ **Limitation des finalités :** Vous devez collecter des données personnelles qu'à des fins légitimes et spécifiques. Indiquez clairement quelles sont ces raisons et conservez les données uniquement pour la durée nécessaire à la finalité visée.

- ✓ **Minimisation des données :** Vous ne pouvez traiter des données à caractère personnel que si cela est strictement nécessaire pour répondre aux finalités spécifiques pour lesquelles elles ont été collectées. Cela représente deux principaux avantages. Premièrement, en cas de violation de données, toute personne non-autorisée ayant accès aux données ne pourra voir qu'une quantité limitée de données. Deuxièmement, la minimisation des données permet de préserver l'exactitude des données et d'assurer leur mise à jour.

- ✓ **Exactitude et mise à jour des données :** L'exactitude des données personnelles fait partie intégrante de la notion de protection des données. Le RGPD indique que toutes les mesures raisonnables doivent être prises afin de supprimer ou de modifier les données inexactes ou incomplètes.

[4] Article 5 du RGPD.

- ✓ **Limitation de la durée de conservation des données :** De la même façon, vous devez supprimer les données personnelles qui ne sont plus nécessaires pour répondre aux finalités pour lesquelles elles ont été collectées.

- ✓ **Intégrité et confidentialité :** Vous devez prendre toutes les précautions utiles pour protéger les données de vos patients contre tout accès non autorisé ou illicite et contre la perte, la destruction ou les dégâts d'origine accidentelle.

- ✓ **Responsabilité (« *accountability* ») :** Vous devez garantir le respect des principes énoncés ci-dessus et être à même de démontrer que vos traitements sont en conformité avec ces grands principes. Veillez donc à bien **documenter votre mise en conformité**.

2. Informer vos patients et s'assurer du respect de leurs droits

Vous devez **informer vos patients que leurs données personnelles sont recueillies et traitées en conformité avec le RGPD en vue d'assurer une prise en charge optimale de leur santé**. Vous devez également informer vos patients que leurs données sont utilisées par toute ou partie de l'équipe mono ou pluridisciplinaire dans le respect du secret professionnel en vue d'adopter une **approche globale coordonnée intégrant soins, démarches préventives de santé et suivi médico-social.** Cette information peut se faire par la voie d'affichage dans la salle d'attente, ou par la remise d'un dépliant au patient.

L'information doit comporter impérativement les éléments suivants :

- les coordonnées du ou des responsables de traitement
- les finalités visées y compris les finalités ultérieures *(si un prestataire de soins souhaite utiliser ultérieurement les données à des fins de recherche par exemple*)
- les destinataires des données
- la durée de conservation des données
- les droits de la personne: droit d'accès et de copie, droit à la rectification et à l'effacement des données (sous certaines conditions), droit à la limitation du traitement des données, droit d'opposition (sous certaines conditions) et droit de porter plainte auprès de l'autorité de protection des données (APD)

★ Téléchargez vite votre affiche sur www.e-santewallonie.be

3. Tenir un registre des activités de traitement

Chaque responsable de traitement doit tenir un registre des activités de traitement[5].

[5] Article 30 du RGPD.

★ Pour plus d'informations, voyez la « Fiche 1. Le registre des activités de traitements » disponible sur www.e-santewallonie.be

4. Désigner une personne référente pour la protection des données

Si vous exercez votre activité professionnelle en « solo », vous n'êtes pas soumis à l'obligation de désigner un délégué à la protection des données (DPO)[6].

En revanche, si vous exercez votre activité de soins en groupe, **la désignation d'une personne référente pour la protection des données est vivement encouragée**. Cette personne pourrait être en charge notamment de :

- **sensibiliser** l'équipe de soins et les autres membres du cabinet à la protection des données
- **tenir et à mettre à jour le registre** des activités de traitement
- être la personne de référence pour toutes **questions relatives à la protection des données** (demande d'accès, de rectification de suppression des données)
- être la personne de référence pour **centraliser les fuites de données** et en faire **rapport à l'Autorité de Protection des Données (APD)**.

5. Sécuriser les échanges de données à caractère personnel

En tant que responsable de traitement des données, vous êtes tenu de respecter les règles de sécurité.

La principale mesure de sécurisation des données est **la prise de bonnes habitudes**. Ces dernières sont simples et ne coûtent rien. *Par exemple : fermer les portes où les dossiers patients sont conservés à clé, ne pas laisser des mots de passe à vue et ne pas les communiquer, ne pas jeter de protocoles dans la poubelle du couloir, envoyer les rapports médicaux sous cachet « confidentiel »…*

Ensuite, des **mesures de sécurité plus techniques** peuvent être prises pour les locaux. Par exemple : *utilisation de badges électroniques avec des accès personnalisés selon les profils de professionnels, systèmes d'alarme, système de vidéosurveillance...*

6. Vous devez conclure un contrat de sous-traitance avec vos prestataires

Si vous utilisez un logiciel dans le cadre de votre pratique pour la gestion des dossiers patients, si vous utilisez un agenda en ligne, si vous recourrez à un cloud ou si vous faites

[6] Article 37 du RGPD.

appel à des services externes de tarification, il est de votre responsabilité de vérifier que votre prestataire répond également aux exigences du RGPD et fournit des garanties suffisantes en termes de sécurité et de confidentialité des données, via la conclusion d'un **contrat de sous-traitance conforme à l'article 28 du RGPD**.

★ Pour plus d'informations, voyez la « Fiche 4. Les contrats de sous-traitance» disponible sur www.e-santewallonie.be

7. Notifier à l'Autorité de Protection des Données (APD) toute violation des données et tenir un registre des incidents

Vous devez **prendre toutes les précautions utiles pour empêcher que des tiers non autorisés aient accès aux données de vos patients, de vos collaborateurs et du personnel.**

Si vous constatez une violation de données[7] comportant un risque pour les droits et les libertés des personnes concernées, vous devez en informer dans les 72 heures l'autorité de protection des données (APD). Si le risque est élevé, vous devez également en informer les personnes concernées.

Toute violation de données doit être documentée dans un **registre des incidents**, tenu à la disposition de l'APD.

★ Pour plus d'informations, voyez la « Fiche 7. Notification des fuites de données» disponible sur www.e-santewallonie.be

Quelles sont les caractéristiques de la responsabilité conjointe ?

1. Vous devez définir vos obligations respectives dans une convention

Le RGPD précise que « *les responsables conjoints du traitement **définissent de manière transparente leurs obligations respectives**, notamment en ce qui concerne l'exercice des droits de la personne concernée et leurs obligations respectives quant à la communication des informations visées aux articles 13 et 14, **par voie d'accord entre eux*** »[8].

Cet accord mutuel devra préciser l'identité des responsables conjoints et définir les obligations de chacun : qui tiendra à jour le registre des activités de traitement, qui est responsable de notifier les fuites de données à l'autorité de protection des données, qui approuvera les demandes de consultation introduites par les patients (dans ce cadre, une personne de contact peut être désignée), etc.

[7] Article 4, 12° du RGPD : « 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 (…) ou l'accès non autorisé à de telles données ».
[8] Article 26 du RGPD.

2. Les grandes lignes de cet accord doivent être mises à la disposition des personnes concernées

Cette formulation semble indiquer que les responsables conjoints n'ont pas l'obligation de communiquer activement ces informations à la personne concernée, mais simplement de **les rendre disponibles**, par exemple par voie d'affichage dans leur salle d'attente ou sur leur site internet.

3. Indépendamment des termes de l'accord, vous êtes chacun tenu solidairement à l'égard de la personne concernée.

En dépit de cet accord mutuel, chaque responsable de traitement assume *in fine* la responsabilité afférente à ses obligations et peut donc être interpellé au sujet du (non-) respect du RGPD. Le RGPD instaure une **responsabilité solidaire** entre les responsables conjoints vis-à-vis de la personne concernée.

Si la violation du RGPD entraine un préjudicie pour la personne concernée, un responsable conjoint ne peut échapper à sa responsabilité que s'il est en mesure de démontrer qu'il n'est nullement responsable du fait générateur du préjudice.

Quelles sont vos sanctions en cas de non-respect du RGPD ?

Le non-respect du RGPD peut s'accompagner de **sanctions pénales ou financières particulièrement dissuasives**[9].

Nonobstant, l'Autorité de Protection des Données (APD) peut préférer vous imposer d'adopter des **mesures correctrices** (par exemple, mise en conformité dans un délai déterminé, limitation de traitement, rectification ou effacement de données).

L'essentiel est donc de pouvoir démontrer dès à présent à l'APD que vous vous êtes engagé dans une démarche sérieuse de mise en conformité.

Pour e-santewallonie,

Emeraude Camberlin, Juriste.

[9] Article 83 du RGPD