# Fiche 3.

## La pratique de groupe

***Check-list des bonnes pratiques à respecter :***

→ Je respecte les grands principes de protection des données ;

→ J'informe mes patients et m'assure du respect de leurs droits (Téléchargez vite votre affiche sur www.e-santewallonie.be) ;

→ Je tiens un registre à jour de mes activités de traitement des données (Téléchargez le registre sur www.e-santewallonie.be) ;

→ Je désigne une personne référente pour la protection des données ;

→ Je réalise une analyse d'impact des risques ;

→ Je mets en place des mesures de sécurité adéquates ;

→ Je veille à conclure un contrat de sous-traitance avec les prestataires de service ;

→ Je notifie toute violation de données à l'Autorité de Protection des Données (ADP) et je tiens un registre des incidents ;

→ Si je suis responsable conjoint, je veille à formaliser mes relations dans une convention.

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 seront atteints.

## 3. Plusieurs cas de figure

### A. Vous exercez seul (comme indépendant) votre activité professionnelle

Dans ce premier cas de figure, **vous êtes considéré comme responsable de traitement**. C'est vous qui définissez les finalités et les moyens de traitement des données de vos patients. Vous devez donc vous assurer de la mise en œuvre des exigences et des obligations du RGPD.

### B. Vous exercez comme indépendant au sein d'une entité mono ou pluridisciplinaire

Si vous exercez comme indépendant au sein d'une maison médicale ou d'un cabinet de kinésithérapeutes par exemple, deux hypothèses doivent être distinguées :

- **Si vous tenez vos dossiers patients via un système propre indépendant 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.

- **Si les moyens alloués à la tenue de vos dossiers patients sont définis par l'entité juridique sous laquelle vous exercez votre mission de soins** (vous travaillez sur un « logiciel métier » commun mis à votre disposition par l'entité juridique), vous êtes considéré comme **responsable CONJOINT** (étant entendu que l'autre responsable conjoint est l'entité juridique). Puisque vous partagez les mêmes finalités et moyens de traitement des données de vos patients, vous devez veiller ensemble à la mise en œuvre des exigences et obligations du RGPD en tenant compte des spécificités liées au régime de la responsabilité conjointe.

### C. Vous exercez comme indépendant en partie au sein d'une entité mono ou pluridisciplinaire et en partie dans un cabinet privé

Si vous exercez votre activité professionnelle en partie dans une maison médicale par exemple 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 de la maison médicale à laquelle 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 diffèrent, les garanties de protection que vous accordez aux données de vos patients restent elles identiques.

### D. Vous exercez comme salarié au sein d'une entité mono ou pluridisciplinaire

Lorsque vous êtes engagé en tant que salarié au sein d'une entité mono ou pluridisciplinaire, vous n'êtes **PAS considéré comme responsable de traitement**. C'est **l'entité juridique** sous laquelle vous travaillez qui est juridiquement désignée comme responsable de traitement et sera donc responsable de la mise en œuvre des exigences et des obligations du RGPD.

Bien que vous ne soyez pas responsable de traitement au sens du RGPD, il est néanmoins de votre responsabilité de vous conformer aux exigences déontologiques et légales auxquelles votre profession est soumise (devoir d'information, obligation de confidentialité, accès au dossier patient, tenue d'un dossier patient à jour et conservé dans un lieu sûr, recueil d'un consentement libre, spécifique et éclairé pour l'échange électronique des données, etc.). Par conséquent, il vous importe aussi de tenir compte dans votre pratique des grands principes relatifs à la protection des données à caractère personnel. Ainsi, dans une certaine mesure, **vous participez à la mise en conformité de votre pratique professionnelle avec le RGPD**.

## Quelles sont vos obligations respectives ?

Une fois identifiés, 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[3]:

- ✓ **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.

[3] Article 5 du RGPD.

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

- ✓ **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.

- ✓ **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 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 voie d'affichage dans la salle d'attente, ou par la remise d'un dépliant au patient par exemple.

L'information doit comporter impérativement les éléments suivants :

- les coordonnées du responsable de traitement
- les finalités y compris les finalités ultérieures (*ex : si un prestataire de soins souhaite utiliser ultérieurement les données à des fins de recherche*)
- les destinataires des données
- la durée de conservation
- les droits de la personne concernée : accès, rectification, effacement (sous certaines conditions), limitation, opposition 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[4].

★ 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)[5].

En revanche, si vous exercez votre activité 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)**.

[4] Article 30 du RGPD.
[5] Article 37 du RGPD.

## 5. Réaliser une analyse d'impact des risques [6]

Le traitement de données de santé peut avoir des impacts non négligeables sur la vie privée et les droits et libertés de vos patients. C'est pourquoi le RGPD impose aux responsables du traitement de réaliser une **analyse d'impact sur le traitement de ce type de données**. Cette analyse doit contenir[7] :

- Une description des opérations de traitement envisagées et les finalités poursuivies
- Une évaluation de la nécessité et de la proportionnalité des opération de traitement au regard des finalités poursuivies
- Une évaluation de l'intérêt au regard des risques (bénéfices/risques) notamment au regard des droits et libertés fondamentaux reconnus aux patients. Le traitement de données sensibles présente un intérêt majeur pour les patients au regard des risques encourus en cas de fuite ou de vol de ces données.
- Les mesures de protections mises en place pour limiter les risques (anonymisation, certificat ehealth, cryptage des données…)

## 6. 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 une enveloppe fermée…*

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...*

## 7. Vous devez conclure un contrat de sous-traitance avec vos prestataires [8]

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 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**.

[6] Un modèle d'analyse d'impact des risques vous sera proposé ultérieurement.
[7] Article 35 du RGPD.
[8] Une fiche pratique sera prochainement consacrée aux contrats de sous-traitance RGPD.

### 8. 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[9] 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[10].

## 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*** »[11].

**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 achètera le logiciel de sécurisation nécessaire, qui approuvera les demandes de consultation introduites par les patients (dans ce cadre, une personne de contact peut être désignée), etc[12].

### 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.

[9] 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 ».
[10] Une fiche pratique sur ce thème sera prochainement publiée sur le site esantewallonie.be
[11] Article 26 du RGPD.
[12] Un modèle de convention vous sera proposé ultérieurement.

### 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**[13].

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.**

Par Emeraude Camberlin, Juriste.

[13] Article 83 du RGPD : En fonction de la gravité du non-respect de la réglementation, des amendes administratives allant jusqu'à 20 millions d'euros ou 4% du chiffre d'affaires annuel. Quant aux peines pénales maximales, elles sont, pour une personne physique, de 5 ans d'emprisonnement et de 300.000 d'euros d'amende et, pour une personne morale, de 1,5 millions d'euros d'amende.