Fiche 4.

Les contrats de sous-traitance

Check-list des bonnes pratiques à respecter :

→ J'identifie dans mon registre des traitements les sous-traitants qui interviennent sur chaque traitement de données ;

→ Je fais appel uniquement à des sous-traitants présentant des garanties suffisantes pour la protection des données de mes patients et je veille à l'effectivité des garanties offertes par le sous-traitant;

→ Je fournis des instructions documentées par écrit à mon sous-traitant pour qu'il puisse agir selon celles-ci ;

→ Je veille à la licéité des traitements de données en ce compris des transferts de données vers des pays situés hors de l'Union européenne ;

→ Je conclus avec mes sous-traitants un contrat relatif au traitement de données présentant l'ensemble des mentions obligatoires de l'article 28 du RGPD ;

→ J'analyse et révise mes contrats en cours.

Depuis l'entrée en vigueur du RGPD, les responsables de traitement ainsi que leurs sous-traitants se voient imposer un certain nombre d'obligations dont découlent certaines responsabilités.

C'est pourquoi il est primordial que vous **identifiez vos relations de sous-traitance** et que vous **qualifiez précisément le rôle de chacun des acteurs intervenant sur les différents traitements de données à caractère personnel.**

Vous devez ainsi être en mesure de **déterminer si le destinataire des données à caractère personnel agit en tant que responsable de traitement ou en tant que sous-traitants.**

Définitions

1. Responsable du traitement

Pour rappel, le RGPD définit le responsable de 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 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 ?

Dans le cadre de l'exercice de votre activité professionnelle, **vous** êtes désigné comme le **responsable des données personnelles** que vous collectez ou émettez tantôt sur vos patients tantôt sur les membres de votre personnel.

2. Sous-traitant

Au sens du RGPD, il y a lieu d'entendre par sous-traitant toute « ***personne physique ou morale, autorité publique, agence ou autre organisme qui, traite des données à caractère personnel pour le compte du responsable de traitement*** »[2].

Trois éléments ressortent de cette définition. Un sous-traitant est :
- toute entité (autre que le responsable de traitement)
- qui traite des données à caractère personnel
- pour votre compte (c'est-à-dire dans votre intérêt)

[1] Article 4, 7° du RGPD.
[2] Article 4, 8° du RGPD.

A ces trois éléments constitutifs de la notion de sous-traitant s'ajoute le fait qu'**un sous-traitant ne traite des données à caractère personnel que sur instructions du responsable de traitement**[3].

Cette notion est donc à rapprocher de la notion usuelle de la sous-traitance telle que reprise dans le dictionnaire Larousse : « *opération par laquelle un entrepreneur confie, **sous sa responsabilité et sous son contrôle**, à une autre personne (sous-traitant) tout ou partie de l'exécution des tâches qui sont à sa charge* ».

Le critère déterminant pour la qualification de sous-traitant est donc **l'existence d'un contrôle et d'instructions données** par le responsable de traitement (c'est-à-dire, vous).

A noter toutefois qu'une certaine **marge de manœuvre** peut être laissée au sous-traitant concernant les moyens à mettre en œuvre pour traiter les données personnelles (à savoir le « **comment** »). C'est particulièrement vrai lorsque le responsable de traitement fait appel à un prestataire spécialisé dans un domaine précis. Les instructions seront nécessairement limitées mais le contrôle lui demeure.

A partir de ces éléments constitutifs de la définition de sous-traitance, vous devez donc être **capables d'identifier dans votre registre des activités de traitement les différents sous-traitants qui interviennent sur chaque traitement de données à caractère personnel**.

Qui sont vos sous-traitants ?

Il n'est pas toujours évident de déterminer si le destinataire des données est qualifié de responsable de traitement ou de sous-traitant. Pour cela, une série d'indices peut être utilisées, toujours en partant d'une **analyse au cas par cas**.

TRUC ET ASTUCE pour vous aider à identifier vos sous-traitants :

Dès que vous faites appel à un **service** (*une tâche bien précise*) **ou une prestation** (*un service plus étendu*) **que vous pouvez réaliser vous-mêmes mais que vous décidez de confier à un tiers sous votre responsabilité et conformément à vos instructions** (*ex : la configuration d'un logiciel métier pour la tenue des dossiers de vos patients*), ce prestataire de service répond à la définition de **sous-traitant**.

Plus **le niveau d'instructions** données au prestataire de service est important, plus on se trouve face à un rapport de sous-traitance.

[3] Article 28 du RGPD.

SONT vos sous-traitants (*liste non exhaustive*) :

- Votre **logiciel métier**
- Le **Réseau Santé Wallon** (RSW)
- Les sociétés qui vous offrent un **service d'agenda en ligne**
- Les sociétés de **facturation**
- Les sociétés **d'hébergement des données de type *Cloud SaaS***
- Les sociétés offrant un service de **messagerie électronique**
- **…**

NE SONT PAS vos sous-traitants :

- **Votre secrétaire médical**, bien qu'il agisse sous votre responsabilité directe, n'est pas votre sous-traitant car il appartient à la même entité juridique que vous ;
- Un **fournisseur de service qui ne traiterait pas de données à caractère personnel** pour votre compte (*ex : simple location ou vente d'outils informatiques*) ne pourra pas non plus être considéré comme votre sous-traitant ;
- Vos **confrères spécialistes** vers lesquels vous renvoyez vos patients ne rentrent pas dans la définition de « sous-traitant ». Ils sont considérés comme des responsables de traitement, au même titre que vous. En effet, ils ne traitent pas de données personnelles pour votre compte et selon vos instructions, ils traitent votre demande de manière autonome, en déterminant les finalités et les moyens de traitement nécessaires pour l'exercice de leur activité professionnelle.

Si vous êtes amené, en vertu d'une obligation légale, à travailler avec un prestataire de service identifié (*ex : MyCareNet, Sciensano…*), ce dernier sera considéré comme un « **responsable du traitement** ». C'est en effet lui qui détermine les finalités et les moyens de traitement des données. Et vous, vous êtes l' « **utilisateur final** » d'un service mis à votre disposition.

Quelles sont vos obligations en tant que responsable de traitement vis-à-vis de vos sous-traitants ?

Le RGPD impose une série d'obligations aux responsables de traitements dans leurs relations avec leurs sous-traitants.

1. Vous devez faire appel uniquement à des sous-traitants présentant des garanties suffisantes en terme de protection des données.

Le sous-traitant à qui vous confiez en tout ou en partie la gestion des données à caractère personnel de vos patients doit vous offrir des **garanties suffisantes pour la protection de ces données**, que ce soit au niveau de leurs connaissances, de leurs ressources ou de leur fiabilité.

De sorte que vous puissiez raisonnablement vous assurer de l'effectivité des garanties que votre sous-traitant offre en matière de protection des données, vous pouvez exiger de lui qu'il vous communique **une description écrite et détaillée des mesures de sécurité (techniques ou organisationnelles) mises en place** pour garantir que le traitement des données personnelles respecte bien les exigences du RGPD et assure les droits des personnes concernées.

Bien souvent, les garanties offertes par les sous-traitants sont les suivantes :

- le chiffrement des données selon leur sensibilité ou à défaut l'existence de procédures garantissant que le sous-traitant n'a pas accès aux données qui lui sont confiées ;
- le chiffrement des transmissions de données (*ex : connexion de type HTTPS, VPN, etc.*) ;
- des garanties en matière de protection du réseau, de traçabilité (*journaux, audits*), de gestion des habilitations, d'authentification ;
- la copie de sauvegardes ;
- l'anonymisation ou la pseudonymisation des données ;
- la détention de certifications ISO ou autres ;
- l'existence d'un code de conduite conforme aux articles 40 ou 42 du RGPD ;
- etc.

En pratique, le niveau d'exigence que vous pouvez exiger de votre sous-traitant dépendra de ses ressources, qu'elles soient humaines, matérielles ou techniques.

2. Vous devez fournir des instructions spécialement documentées.

En tant que responsable du traitement, c'est à vous de définir les finalités et les moyens du traitement des données. C'est à vous de décider **POURQUOI** vous collectez telles données sur votre patient et **COMMENT** vous allez le faire.

Votre sous-traitant agit uniquement sur base de vos instructions. Cela ne veut pas pour autant dire que votre sous-traitant devra rester passif. Il dispose en effet, en vertu de son expertise en matière de protection des données, d'une certaine marge de manœuvre dans les moyens du traitement des données à mettre en place pour servir vos intérêts et ceux de vos patients.

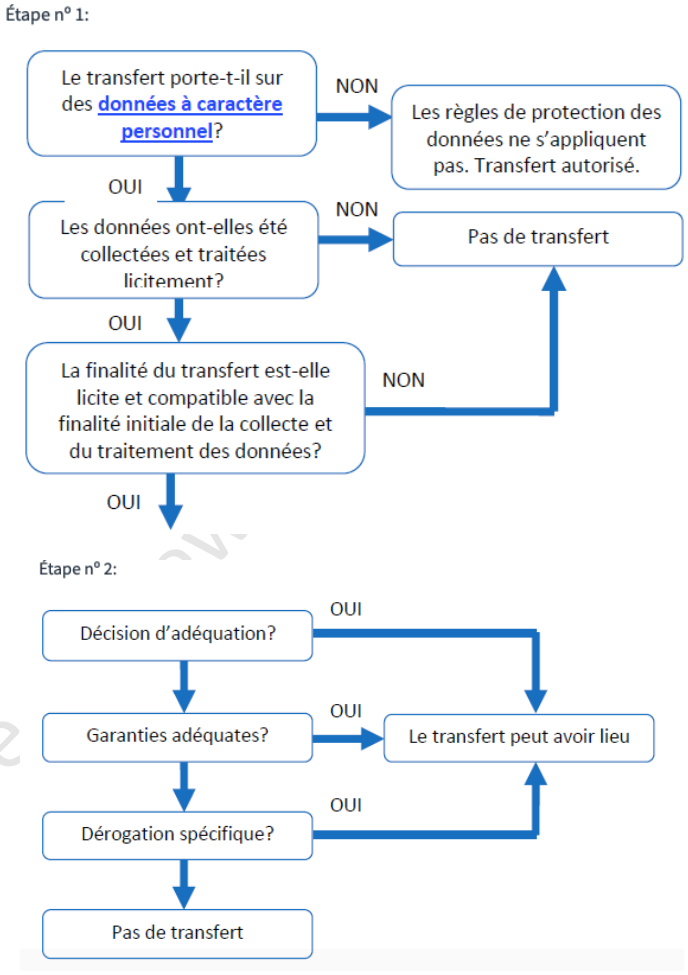
3. Vous devez vous assurer de la licéité des traitements de données en ce compris des transferts de données hors de l'Union européenne.

De manière générale, vous devez prendre toutes les mesures appropriées pour assurer mais aussi pour démontrer en vertu du principe *« accountability »,* que le traitement des données est conforme aux exigences du RGPD. Ainsi, assurez-vous que votre sous-traitant respecte lui aussi l'ensemble des exigences du RGPD.

Attention aux transferts de données hors de l'UE !!!

Il faut savoir qu'à l'heure actuelle l'Union européenne bénéficie du meilleur système juridique en termes de protection des données à caractère personnel. Par conséquent, **si des radios, des diagnostics ou encore des études cliniques sont envoyées hors de l'Union européenne,** vous devez vérifier que le **pays destinataire offre des garanties équivalentes à celles instaurées dans le RGPD**[4].En pratique :

- Soit le pays tiers (située hors de l'UE) a reçu une décision d'adéquation de la Commission européenne[5] (ex : Israël, Japon, Suisse, Argentine…) dans ce cas vous pouvez envoyez les données sans formalité particulière.
- Soit le pays tiers n'a pas reçu de décision d'adéquation, dans ce cas, vous devez veiller à des garanties contractuelles et notamment la signature des Clauses Contractuelles Types de la Commission européenne[6] ;



[4] Cfr. articles 44 et 45 du RGPD.

[5] Cfr. liste officielle des pays ayant reçu une décision d'adéquation de la Commission européenne : https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en

[6] Clauses Contractuelles Types de la Commission européenne : https://www.autoriteprotectiondonnees.be/en-dehors-ue-sans-protection-adequate-clauses-contractuelles

4. Vous devez prévoir un contrat de sous-traitance avec vos différents sous-traitants conforme aux mentions de l'article 28 du RGPD.

En toute hypothèse, dès que vous sollicitez les services d'un sous-traitant (*société de maintenance, hébergeur de données de santé, webservice*…) vous devez **formaliser la relation que vous entretenez avec lui par un contrat de sous-traitance.**

Ce contrat doit contenir une série de mentions **obligatoires** qui peuvent être classées en deux catégories : les mentions d'ordre général et la description des obligations du sous-traitant.

Pour les **mentions d'ordre général**, le contrat détermine :

- **l'objet** et **la durée** du traitement des données ;
- **sa nature** (par exemple, enregistrer des données, les comparer…) et **sa finalité** (objectif principal du traitement : par exemple, gestion efficace du suivi médical du patient …) ;
- le **type de données** traitées (données d'identification ou données sensibles) ;
- les **catégories de personnes concernées** (patients, famille du patient, participants à une étude clinique …) ;
- les **obligations et les droits du responsable du traitement**.

Remarque : Ces mentions figurent le plus souvent dans une **annexe** au contrat. Veillez donc bien à la lire, à émettre vos commentaires et à la compléter si nécessaire.

En ce qui concerne **la description des obligations du sous-traitant**, le contrat doit obligatoirement mentionner que le sous-traitant :

1. ne traite les données à caractère personnel que sur **vos instructions** ;
2. veille à la signature d'engagements de **confidentialité** par le personnel (modalités en fonction de la sensibilité des données);
3. prend toutes les **mesures de sécurité adéquates** (chiffrement, pseudonymisation, plan de reprise des activités, copies de sauvegarde…);
4. ne recrute pas de sous-traitant sans votre **autorisation** écrite préalable ;
5. **coopère avec vous pour le respect de vos obligations** notamment lorsque des patients ont des demandes concernant l'exercice de leurs droits ;
6. **vous aide à garantir le respect de vos obligations** en matière de notification et de communication de violations de données, d'analyse d'impact et de consultation préalable relative à la protection des données.
7. **supprime ou vous renvoie l'ensemble des données** à caractère personnel à l'issue du contrat ;
8. **met à votre disposition les informations nécessaires** pour démontrer le respect des exigences du RGPD et pour collaborer dans le cadre d'audits.

Tous les contrats de sous-traitance qui sont en cours d'exécution devront nécessairement comprendre ces huit clauses obligatoires.

Passez donc en revue vos différents contrats avec vos sous-traitants qui traitent des données personnelles pour votre compte afin de vérifier qu'ils sont bien conformes au RGPD.

- Des **modèles de clauses** sont disponibles sur le site https://www.cnil.fr/fr/sous-traitance-exemple-de-clauses.

Quelle est votre responsabilité en cas de manquement à vos obligations ?

L'article 82 du RGPD organise une **responsabilité solidaire** entre le responsable de traitement et son sous-traitant.

Ainsi, toute personne qui aurait subi un dommage matériel ou moral du fait d'une violation du RGPD peut obtenir la réparation intégrale de son préjudice tant de la part du responsable de traitement que du sous-traitant.

Une confiance et une coopération mutuelles sont donc d'autant plus indispensables que les sanctions[7] sont partagées, le sous-traitant pourra être contrôlé et sanctionné par l'Autorité de Protection des Données (APD) au même titre que l'est le responsable de traitement.

Pour e-santéwallonie,
Emeraude Camberlin, Juriste.

[7] Cfr. article 83 du RGPD.