Fiche 1.

Le registre des activités de traitement

Check-list des bonnes pratiques à respecter :

→ Je recense de façon précise les traitements de données à caractère personnel que je fais dans le cadre de mon activité professionnelle ;

→ Pour chaque traitement de données, j'indique la finalité du traitement, les catégories de données concernées, les personnes concernées, les durées de conservation, les destinataires, en ce compris les sous-traitants auxquels je fais appel et une description des mesures de sécurité prises ;

→ Je me pose les bonnes questions ;

→ Je tiens à jour régulièrement mon registre ;

→ Je conserve mon registre en interne et je le mets à la disposition de l'autorité de protection des données (APD) à la première demande de celle-ci.

Cette fiche s'adresse principalement aux prestataires de la première ligne de soins, qui exercent leur activité libérale à titre individuel ou en pratique de groupe, à l'exclusion du milieu hospitalier où l'institution hospitalière endosse la responsabilité des opérations de traitement des données effectuées par les personnes qui la composent.

Cette fiche n'a pas pour ambition d'être exhaustive mais a pour ambition d'apporter des pistes et clés de lecture pour les prestataires de soins qui doivent se conformer avec les exigences de la nouvelle Réglementation générale relative à la protection des données (RGPD). Chaque prestataire de soins reste tenu d'évaluer sa mise en conformité avec ledit RGPD. Le respect des exigences du RGPD se fait sous l'entière responsabilité du prestataire de soins et n'engage d'aucune manière la responsabilité du projet e-santewallonie.

Pour plus d'informations : questionsrgpd@e-santewallonie.be

Pourquoi établir un registre des activités de traitement ?

La tenue d'un registre des activités de traitement est une **nouvelle obligation** prévue par **l'article 30 du RGPD**[1].

Sont toutefois exemptés de cette obligation les organisations ou entreprises qui comptent moins de 250 employés. Si *a priori* cette exemption semble bien large, il n'en est rien. En effet, elle ne vaut plus si le traitement mis en œuvre est susceptible de comporter un risque pour les droits et les libertés des personnes concernées, s'il n'est pas occasionnel ou s'il porte notamment sur des données sensibles.

Puisque vous collectez ou émettez des données sensibles sur vos patients et que vous traitez les données personnelles de vos fournisseurs et de votre personnel de façon régulière dans le cadre de votre activité professionnelle, **vous êtes soumis individuellement à l'obligation de tenir un registre des activités de traitement des données** dont vous disposez.

Le registre « RGPD », un outil essentiel de conformité !

Au-delà de la réponse à l'obligation prévue par **l'article 30 du RGPD**, le registre est un outil de pilotage et de démonstration de votre conformité au RGPD. Il doit vous permettre de **recenser les différentes activités de traitement de données personnelles** que vous réalisez dans le cadre de votre mission de soins et de **disposer d'une vue d'ensemble de ce que vous faites avec ces données.**

Lors de la tenue de ce registre, vous devez être attentifs à garder à l'esprit l'ensemble des principes directeurs inscrits à **l'article 5 du RGPD** et plus particulièrement les principes de **licéité** du traitement, de **pertinence** et de **minimisation** des données, d'**exactitude** et de la limitation de la **conservation** des données.

Ainsi, prenez la peine de vous **poser les bonnes questions** : Suis-je légitimement autorisé à traiter les données personnelles de la personne concernée ? Ai-je vraiment besoin de cette donnée dans le cadre de mon activité professionnelle ? Est-il pertinent que je conserve aussi longtemps toutes les données ? Suis-je autorisé à transmettre les données de mes patients ? Les données que je traite sont-elles suffisamment protégées ? Etc.

Le registre « RGPD » peut donc être vu comme **un document interne essentiel devant faciliter la mise en conformité des traitements de données que vous opérez avec les exigences du RGPD.**

[1] L'obligation de déclaration préalable des traitements auprès de l'ex-Commission vie privée, telle qu'elle était prévue sous la LVP de 1992, disparaît au profit de cette nouvelle obligation.

Quelles informations doit contenir le registre ?

Le registre des activités de traitement doit refléter la réalité de vos traitements de données personnelles et vous permettre d'identifier précisément :

- **Vos coordonnées** et celles du référent à la protection des données que vous avez préalablement désigné au sein de votre établissement.
- **Les catégories de données que vous traitez** :

  - **Données d'identification** : nom, prénom, numéro de registre national, date de naissance, adresse, numéro de téléphone, email ;
  - **Données de santé** : historique médical, historique des soins, diagnostics médicaux, traitements prescrits, nature des actes effectués, résultats d'examens de biologie médicale et tout élément de nature à caractériser la santé du patient, informations relatives aux habitudes de vie et de consommation si elles sont collectées avec l'accord du patient et dans la stricte mesure où elles sont nécessaires aux diagnostics et aux soins ;
  - **Autres catégories de données** : données d'assurabilité, particularités financières, loisirs et intérêts, habitudes de vie, profession, emploi, conditions de travail, contexte familial, … (dans la mesure de ce qui est strictement nécessaire).

- **La finalité du traitement des données** (= *à quoi servent les données que vous traitez* ?). La description de la finalité du traitement doit être la plus précise que possible. Il ne peut y avoir de traitement caché.
- **Les catégories de personnes concernées** : patient, famille du patient, autre prestataire de soins, personnel, fournisseur.
- **Les catégories de destinataires** auxquels les données à caractère personnel ont été ou seront communiquées (le patient lui-même ou son représentant légal, un organisme tiers, un autre prestataire de soins, une autorité compétente…) , y compris les sous-traitants auxquels vous recourez (Réseau Santé Wallon, fournisseur de votre logiciel métier…) .
- Si un transfert de données est réalisé dans un pays situé hors de l'Union européenne, il est important d'indiquer les garanties de protection appropriées qui existent.
- **Les durées de conservation des données** (= *combien de temps vous les conservez* ?).
- Dans la mesure du possible, **une description des mesures techniques et organisationnelles** (= *comment sont-elles sécurisées* ? Ex : Back-up, firewall, accès aux locaux via des badges…)

Puisque le registre des activités de traitement est un outil interne d'aide à la mise en conformité avec le RGPD, **il peut contenir toutes les informations complémentaires que vous jugez utiles d'y faire figurer** comme par exemple la mention de la base légale du traitement, les supports utilisés ou encore le degré de probabilité et de gravité d'une fuite des données.

Quelle forme doit prendre ce registre ? Comment l'établir ?

Le format du registre est libre mais doit nécessairement se présenter sous une forme **écrite.**

Vous pouvez donc décider de tenir votre registre de traitement sous un format papier ou utiliser un format électronique (fichier word, excel ou autre logiciel spécifique) tant que sa lecture est suffisamment **claire** et **compréhensible** pour l'Autorité de Protection des Données (APD) en Belgique.

Le registre ne doit toutefois pas exister à la fois en version papier et en version électronique.

A quelle fréquence faut-il mettre à jour le registre ?

Le registre doit être **mis à jour régulièrement** au gré des évolutions fonctionnelles et techniques des traitements de données que vous opérez.

En pratique, toute modification apportée aux conditions de mise en œuvre de chaque traitement (nouvelle donnée collectée, allongement de la durée de conservation, nouveau destinataire du traitement, nouvelle mesure de sécurité, etc.) doit figurer dans le registre.

Dans ce cadre, il peut être utile d'**indiquer la date de la dernière mise à jour réalisée.**

A qui ce registre est-il destiné ? Qui peut le consulter ?

Par nature, le registre est un **document interne et évolutif** qui doit avant tout vous aider à piloter votre conformité avec les exigences du RGPD. **Il n'a donc pas vocation à être mis à la disposition du public en ce compris le patient et ses proches.**

Le registre doit toutefois pouvoir être **communiqué à l'autorité de contrôle**, c'est-à-dire l'Autorité de Protection des Données (APD) en Belgique, lorsqu'elle en fait la demande. Elle pourra notamment l'utiliser dans le cadre de sa mission de contrôle des traitements de données opérés.

Quelles sanctions ?

Le non-respect de l'article 30 du RGPD entraine une sanction particulièrement lourde.

L'article 83, §4 du RGPD parle d'une amende administrative pouvant s'élever jusqu'à **10.000.000€** ou, dans le cas d'une entreprise, **jusqu'à 2% du chiffre d'affaires** annuel de l'exercice précédent.

Néanmoins, si l'APD constate un défaut de conformité et vous met en demeure de vous conformer, vous avez encore la possibilité d'adopter les mesures nécessaires pour éviter une sanction. **L'essentiel est de pouvoir démontrer que vous êtes engagés dans une démarche de mise en conformité.**

Proposition d'un modèle de registre RGPD

Pour faciliter votre conformité avec cette nouvelle obligation du RGPD, e-santé Wallonie vous propose **un registre des activités de traitement prérempli**, présenté sous le format d'un fichier Excel, que vous pouvez retrouver sur www.e-santewallonie.be/rgpd.

Ce modèle de registre proposé contient plus d'informations que ce que le RGPD requiert. Il vous permettra de garder une vue d'ensemble sur d'autres informations qui ont également une importance à la lumière des différentes exigences du RGPD.

Toutefois, ce registre des activités de traitement **ne peut être considéré comme exhaustif**. En effet, il a vocation à évoluer et à être amendé au gré des spécificités et des législations auxquelles sont soumis les professionnels de la santé.

Il est à noter également que ce modèle n'est **pas un support officiel** ! Vous êtes donc tout à fait libres de le modifier, le compléter et l'adapter en fonction de votre activité professionnelle personnelle ou encore d'utiliser un autre modèle registre (par exemple un autre logiciel) tant que l'objectif-même du registre est rempli, à savoir **fournir un aperçu complet des traitements de données à caractère personnel opérés**.

N'attendez plus, mettez-vous dès à présent en conformité !

Pour e-santewallonie,

Emeraude Camberlin, Juriste.