Praticia IT

GUIDE GRATUIT · PROFESSIONNELS DE SANTÉ · BELGIQUE

RGPD au cabinet : *la checklist en 10 points.*

Protéger les données de vos patients, sans jargon. Pour les ostéopathes, kinésithérapeutes et autres praticiens.

À cocher en 15 minutes

- 01 ☑ Registre des traitements
- 02 ☑ Information des patients
- 03 ☐ Accord séparé hors soins
- 04 ☐ Collecte minimale
- 05 ☑ Accès verrouillés
- 06 ☐ Appareils chiffrés
- 07 ☑ Sauvegardes testées
- 08 ☐ Prestataires encadrés
- 09 ☐ Échanges sécurisés
- 10 ☐ Conservation & destruction

Frédéric Dubois
Ostéopathe depuis 2005 · fondateur de Praticia IT

praticia.be
Édition novembre 2026

AVANT DE COMMENCER

Le RGPD, ce n'est pas que pour les grandes entreprises

Dossiers patients, bilans, coordonnées, agenda : un cabinet de santé traite chaque jour des **données de santé**. Le RGPD les classe parmi les données « sensibles », qui demandent le plus de précautions.

La bonne nouvelle, c'est que la mise en conformité d'un cabinet tient surtout en quelques réflexes : savoir ce que vous collectez, informer vos patients, sécuriser vos outils et savoir réagir en cas de problème.

Cette checklist reprend les 10 points essentiels. Cochez ce qui est déjà en place, et gardez le reste comme plan d'action.

1. Cochez

Parcourez les 10 points et cochez ce qui est déjà fait dans votre cabinet.

2. Comptez

Faites le total en dernière page pour voir où vous en êtes.

3. Agissez

Commencez par les points non cochés qui vous semblent les plus simples.

Trois notions à connaître

Responsable de traitement : c'est vous. Vous décidez pourquoi et comment les données de vos patients sont utilisées.

Sous-traitant : tout prestataire qui traite ces données pour vous (logiciel en ligne, agenda, hébergeur, informaticien).

APD : l'Autorité de protection des données, l'autorité de contrôle belge du RGPD.

1

Tenez un registre des traitements

C'est la « carte » de vos données : quelles données vous collectez, pourquoi, qui y a accès et combien de temps vous les gardez. Même un cabinet d'une seule personne doit en tenir un, parce qu'il traite des données de santé.

- [ ] J'ai un registre écrit (un simple tableau suffit)
- [ ] Il couvre le dossier patient, l'agenda, la facturation et mes contacts
- [ ] Je peux le présenter si l'APD me le demande

RGPD art. 30 · l'APD propose un modèle de registre sur son site

2

Informez vos patients

Vos patients doivent savoir qui traite leurs données, pourquoi, combien de temps elles sont conservées et quels sont leurs droits (accès, rectification, réclamation auprès de l'APD).

- [ ] Une notice d'information est affichée en salle d'attente ou remise au patient
- [ ] Elle est aussi disponible sur mon site ou ma page de prise de rendez-vous

RGPD art. 13

3

Demandez un accord séparé pour tout ce qui sort des soins

Les données nécessaires aux soins sont couvertes par votre activité de soignant. En revanche, une newsletter, des photos, un témoignage ou un usage publicitaire demandent un **consentement explicite, séparé et révocable**.

- [ ] Je ne mélange pas les données de soins et mes actions de communication
- [ ] Je garde une trace des consentements donnés (et retirés)

RGPD art. 6, 7 et 9

4

Ne collectez que le nécessaire

Chaque information demandée doit avoir une utilité pour la prise en charge ou la gestion du cabinet. Moins de données, c'est moins de risques.

- [ ] Ma fiche d'anamnèse ne contient pas de champs inutiles
- [ ] Je n'enregistre pas de copie de la carte d'identité sans raison

RGPD art. 5 · principe de minimisation

5

Verrouillez l'accès à vos outils

La majorité des incidents viennent d'un mot de passe faible, partagé ou d'un poste resté ouvert entre deux patients.

- [ ] Mots de passe longs et différents pour chaque outil (idéalement via un gestionnaire de mots de passe)
- [ ] Double authentification activée sur la messagerie et le logiciel patients
- [ ] Verrouillage automatique de l'écran après quelques minutes
- [ ] Un compte personnel par utilisateur (pas de compte partagé)

RGPD art. 32 · sécurité du traitement

6

Chiffrez vos appareils

Un ordinateur portable, un téléphone ou une clé USB perdus ne doivent pas permettre de lire vos dossiers.

- [ ] Le disque de mon PC est chiffré (BitLocker sur Windows, FileVault sur Mac)
- [ ] Mon téléphone pro est protégé par un code et chiffré
- [ ] Je n'emporte pas de dossiers sur une clé USB non chiffrée

7

Sauvegardez… et testez vos sauvegardes

Une panne, un vol ou un rançongiciel peuvent effacer des années de dossiers. La règle simple : **3 copies, sur 2 supports différents, dont 1 hors du cabinet**.

- [ ] Mes données sont sauvegardées automatiquement
- [ ] Une copie chiffrée est conservée hors du cabinet
- [ ] J'ai déjà testé une restauration au cours des 6 derniers mois

8

Encadrez vos prestataires

Logiciel en ligne, agenda, hébergement, informaticien : chacun doit s'engager par écrit à protéger vos données.

- [ ] J'ai un contrat ou des conditions de sous-traitance RGPD pour chaque prestataire
- [ ] Je sais dans quel pays mes données sont hébergées (de préférence dans l'Union européenne)

RGPD art. 28

9 Échangez les données de santé par des canaux sécurisés

Un e-mail classique, WhatsApp ou Messenger ne sont pas faits pour transmettre un bilan ou un dossier.

- [ ] J'utilise une messagerie sécurisée pour les échanges entre soignants (par exemple l'eHealthBox, si ma profession y a accès)
- [ ] J'évite d'envoyer des données de santé par e-mail non chiffré ou par messagerie grand public

10 Respectez les durées de conservation, puis détruisez proprement

Pour les professionnels des soins de santé concernés (kinésithérapeutes, médecins…), la loi qualité du 22 avril 2019 impose de conserver le dossier patient **au minimum 30 ans et au maximum 50 ans** après le dernier contact. Les ostéopathes, dont la profession n'est pas encore réglementée en Belgique, vérifieront la règle conseillée par leur union professionnelle.

- [ ] Je connais la durée de conservation qui s'applique à ma profession
- [ ] Les dossiers papier et les anciens disques durs sont détruits de façon sécurisée

RGPD art. 5 · loi du 22 avril 2019 relative à la qualité de la pratique des soins de santé

Et en cas de fuite de données ?

PC volé, piratage, e-mail envoyé au mauvais destinataire… Si l'incident présente un risque pour vos patients, vous devez **le notifier à l'APD dans les 72 heures** après en avoir pris connaissance, et informer les patients concernés si le risque est élevé.

Dans tous les cas, notez l'incident dans un registre des violations : ce qui s'est passé, les conséquences et les mesures prises.

RGPD art. 33 et 34

Faut-il un délégué à la protection des données (DPO) ?

Pour un praticien qui exerce seul, en général non : le RGPD considère que le traitement des données de ses patients par un professionnel de santé individuel n'est pas un traitement « à grande échelle ». Pour un centre ou un cabinet de groupe important, la question mérite d'être posée.

RGPD art. 37 et considérant 91

VOTRE RÉSULTAT

Combien de points avez-vous cochés ?

10 / 10
Bravo, votre cabinet est bien protégé. Pensez à refaire le point chaque année.

6 à 9
Une bonne base. Quelques réglages suffisent pour être serein.

0 à 5
Il est temps d'agir, en commençant par les sauvegardes et les accès.

OFFERT · SANS ENGAGEMENT

Le bilan informatique de votre cabinet

Comme un bilan en consultation, mais pour votre informatique. En 30 minutes, au cabinet ou en visio, on passe en revue votre logiciel, votre matériel, vos sauvegardes et les points RGPD de cette checklist.

Vous repartez avec un rapport clair et des recommandations concrètes, que vous fassiez appel à moi ensuite ou non.

praticia.be **+32 475 86 28 32** **frederic@praticia.be**

Praticia IT, c'est l'informatique de votre cabinet par un praticien : logiciels de cabinet (Oxteo, Kin'Easy, Mobminder), matériel de grandes marques, installation, dépannage et conseil numérique, en Belgique, au Luxembourg et en France.

Ce guide a une vocation pratique et informative. Il ne remplace pas un avis juridique personnalisé. Pour une question précise, consultez l'Autorité de protection des données (autoriteprotectiondonnees.be) ou votre association professionnelle. Informations à jour en novembre 2026.