



REGLEMENT GENERAL DE PROTECTION DES DONNEES

Le Règlement Général de Protection des Données est un règlement européen, à l'attention des entreprises de plus de 250 salariés **et des professionnels de santé**, dont l'objectif est de protéger les personnes de l'utilisation de leurs données. Il entre en application le **25 mai 2018**.

Avec ce règlement, la logique de la protection des données personnelles change. Auparavant, il y avait une obligation de déclarer au préalable à la CNIL l'existence de bases de données personnelles. Désormais, le RGPD inscrit ces questions dans une démarche responsable. Cela signifie que chacun doit questionner ses pratiques et adapter sa conduite.

Cela consiste à se poser les questions suivantes :

- Quelles données suis-je amené à utiliser et stocker ?
- Quel usage vais-je en faire ?
- A qui vais-je transmettre ces données ? Avec qui vais-je les partager ?
- Quels risques fais-je courir à ces données et donc aux personnes concernées ?
- Quelles mesures puis-je mettre en œuvre pour protéger ces données et les personnes qu'elles concernent ?

A cet effet, le guide de la CNIL (dans sa première partie surtout) permet de réfléchir à ces questions et donne des pistes de réponses.

<https://www.cnil.fr/fr/principes-cles/guide-de-la-securite-des-donnees-personnelles> (version site)

https://www.cnil.fr/sites/default/files/atoms/files/cnil_guide_securite_personnelle.pdf (version pdf)

La CNIL a également publié un guide d'action intitulé : 6 étapes pour se préparer au RGPD, qui est plus clair et plus concis. N'hésitez pas à vous y référer et à le suivre pour vous aider dans vos démarches. Le personnel de la CNIL peut également vous renseigner, tout comme votre syndicat professionnel.

<https://www.cnil.fr/fr/principes-cles/rgpd-se-preparer-en-6-etapes>

Voici la marche à suivre recommandée par la CNIL pour aborder cette question :

- Lister les traitements de données à caractère personnel (*quelles données j'utilise et ce que j'en fais*), les données elles-mêmes et les supports sur lesquels elles sont stockées : matériels (ordi, disques durs...), logiciels (de gestion de cabinet...), canaux de communication (internet...), documents papiers
- Apprécier les risques : impacts sur les données (accès illégitime, modification des données, disparition des données), sources de risques (personnes extérieures, risques dans les locaux), menaces réalisables (*est-ce que ça peut m'arriver ?*), mesures existantes ou prévues (*ce que je fais déjà et ce que je vais faire pour protéger les données*), gravité et vraisemblance des risques
- Mettre en œuvre les mesures pour protéger ces informations et vérifier que ces mesures fonctionnent
- Réaliser des "Audits de sécurité" (*vérifier que ça marche bien pour moi*)

Par ailleurs, une démarche individuelle doit être menée auprès de **chaque patient** afin de l'informer au sujet des données personnelles que nous utilisons. Un document doit être signé par chaque patient ou son représentant légal indiquant qu'il ou elle a bien reçu l'information. Vous en trouverez un modèle ci-dessous.

Vous pouvez également afficher l'information en salle d'attente. Néanmoins, si vous avez pris le temps d'informer individuellement chacun de vos patients, cet affichage peut sembler superflu.

Texte à faire signer au patient ou à son représentant légal :

Information sur la collecte de données personnelles

Les informations recueillies par votre orthophoniste (*Prénom, Nom de l'orthophoniste*) sont enregistrées dans un fichier informatisé pour la tenue du dossier patient. Elles seront conservées pendant une durée de 30 ans maximum et sont destinées :

- à l'orthophoniste
- à d'autres professionnels de santé amenés à prendre en charge le patient, pour un partage d'information, avec l'accord du patient et/ou de son représentant légal,
- aux caisses d'assurance maladie et aux mutuelles de l'assuré (essentiellement la télétransmission des feuilles de soins).

Conformément au Règlement Général sur la Protection des Données (RGPD) en vigueur à partir du 25 mai 2018, vous pouvez exercer votre droit d'accès aux données vous concernant, les faire rectifier, effacer, limiter ou vous opposer au traitement en contactant par écrit : *Prénom, Nom et adresse de l'orthophoniste*

A , le

Nom et signature du patient ou de son représentant légal :

Enfin, une dernière obligation du RGPD : vous devez constituer un **registre** indiquant quels types de données vous utilisez et comment vous les protégez. Nous vous transmettons en PJ un modèle à remplir proposé par la CNIL. De nombreux éléments ne seront pas pertinents pour la plupart des orthophonistes. N'hésitez pas à vous aider du site de la CNIL pour le remplir (cf liens donnés plus haut).

En cas de non-respect du RGPD, nous sommes passibles d'une amende dont le montant est égal à 4% de nos recettes.

ATTENTION :

Comme pour les démarches liées à l'accessibilité, vous risquez de subir un démarchage, par téléphone ou par courrier, vous alertant dans des termes inquiétants et vous proposant de réaliser les formalités du RGPD pour vous, en général en échange de sommes considérables. Soyez vigilants, ne payez rien d'emblée et n'hésitez pas à nous contacter en cas de problème.

Quelques notes pour finir :

Vous croiserez dans les documents de la CNIL les initiales NIR pour Numéro d'Inscription au Registre : il s'agit du numéro de Sécurité Sociale.

Pensez à crypter les supports de stockage externes type disque dur externe ou clé usb.

Attention aux comptes partagés, au stockage de données sur cloud/drive/serveur. Lorsque votre logiciel de gestion de cabinet propose ce type de stockage, vérifiez la protection des données.

Pensez à sécuriser vos mots de passe. Voici un guide de la CNIL à ce sujet : <https://www.cnil.fr/fr/les-conseils-de-la-cnil-pour-un-bon-mot-de-passe>

Fédération des Orthophonistes de France
Mai 2018