9 questions/réponses autour du Règlement général sur la protection des données (RGPD)

Maude Premier, *juriste FNO*

Une nouvelle obligation pour tous les cabinets de professionnels de santé libéraux

AVANT LE 25 MAI 2018

1 Qu'est-ce-que le RGPD ?

Le règlement général sur la protection des données est un texte de référence européen en matière de protection des données personnelles pour les résidents de l'Union européenne (UE) applicable à partir du 25 mai 2018.

Le RGPD fixe un nouveau cadre européen pour le traitement et la circulation des données à caractère personnel.

Avant le RGPD, il existait la loi française Informatique et libertés du 6 janvier 1978 qui réglementait le traitement des données personnelles.

2 Quel est l'objectif du RGPD ?

Il vise à harmoniser les données personnelles dans l'ensemble de l'UE.

Le RGDP vise, entre autre, à renforcer les droits des personnes, par la création d'un droit à la portabilité des données personnelles (une personne peut récupérer les données fournies) et de dispositions propres aux personnes mineures (informations sur les traitements claires et simples, consentement du titulaire de l'autorité parentale…).

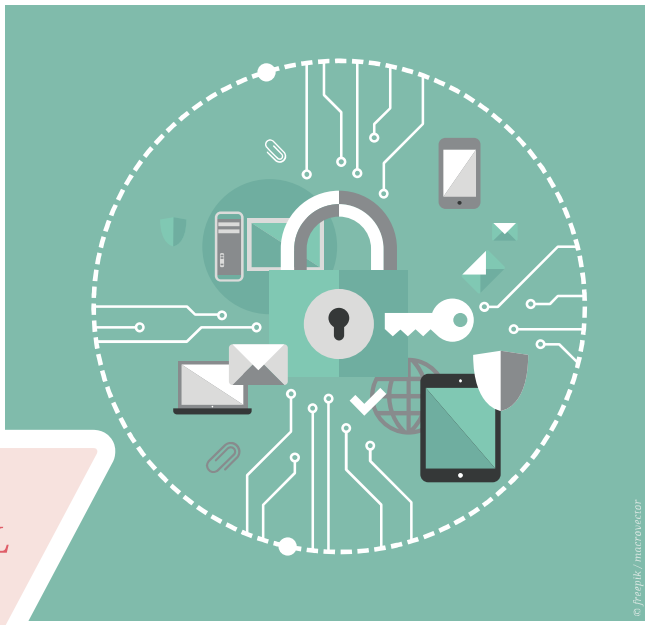
Le RGDP s'applique dès qu'une entreprise, administration, professionnel, etc… traite des données personnelles et ce, quel que soit son secteur d'activité ou son caractère public ou privé.

3 Qu'est-ce qu'une donnée personnelle ?

On entend par données personnelles, **toute information se rapportant à une personne physique identifiée ou identifiable** (nom, prénom, localisation, n° d'identification, photographie, adresse mail...).
Certaines données sont sensibles car elles touchent des informations qui peuvent donner lieu à de la discrimination ou des préjugés (les données de santé, les opinions politique ou religieuses, l'orientation sexuelle, etc...).

4 Date d'entrée en vigueur du RGPD ?

Le RGPD entrera en vigueur **le 25 mai 2018**.
A compter de cette date, **votre cabinet devra se conformer** à cette nouvelle réglementation.



5 Qu'est-ce que le RGPD change pour vous ?

AVEC LE RGPD : plus de déclaration auprès de la CNIL MAIS !! Lisez-la suite...

Vous êtes orthophoniste mais vous êtes aussi usager (les réseaux sociaux, les applications, les montres connectées, les sites internet...) ; vos données personnelles sont en danger et celles de vos patients également, le RGPD permet de réfléchir aux mécanismes de protection à mettre en place.

Pour mémoire, il a fallu du temps pour réaliser que le compte-rendu de bilan orthophonique ne devait plus être envoyé par des messageries non sécurisées, ces données pouvant être facilement récupérées par n'importe qui sur la toile.

Le RGPD met en place un certain nombre de protections : accord préalable avant tout traitement de données personnelles, accord des parents pour qu'un mineur s'inscrive sur un réseau social...
Il existe également un droit à l'oubli qui permet à la personne de demander l'effacement de ses données personnelles en cas d'atteinte à la vie privée.

Au sein de votre cabinet, vous êtes donc concerné puisque vous recueillez des données personnelles sensibles.
Jusqu'à présent, le traitement informatique des données relatives à vos patients nécessitait une déclaration simplifiée auprès de la CNIL.

A partir du 25 mai 2018, vous ne serez plus dans un système déclaratif mais un système responsable.

En effet, le RGPD est basé sur une logique de responsabilisation et de transparence, alors qu'auparavant les obligations imposées par la Loi Informatique et libertés reposaient sur des formalités préalables.

Cela signifie que vous allez devoir réfléchir aux données que vous traitez, à la raison de leur traitement, aux mesures de sécurité, à l'information transmise aux personnes dont les données sont collectées.

Concernant ce dernier point, il faut informer les personnes (patients, assurés sociaux, employés) de la finalité des données collectées et surtout du droit de ces personnes à accéder à leurs données personnelles. En cas de contrôle, il faudra apporter la preuve que vous remplissez bien vos obligations, donc voici un modèle à faire signer aux personnes concernées par le recueil des données personnelles :

Information sur la collecte de données personnelles

Les informations recueillies sont enregistrées dans un fichier informatisé par …… (nom de l'orthophoniste) pour……. (ex : tenue du dossier patient).
Elles sont conservées pendant……..... (ex : durée de conservation du dossier patient 30 ans) et sont destinées …… (ex : à l'orthophoniste ; pour un éventuel partage d'informations avec les professionnels de santé amenés à prendre en charge le patient ; aux caisses/mutuelles de l'assuré social).

Conformément au Règlement général sur la protection des données, vous pouvez exercer votre droit d'accès aux données vous concernant, les faire rectifier, effacer, de limiter ou de vous opposer au traitement en contactant par écrit : …….. (nom de l'orthophoniste).

Date et signature du patient et/ou du représentant légal

Vous pouvez retrouver sur le site de la CNIL le modèle à compléter en ligne :

www.cnil.fr/fr/modele/mention/formulaire-de-collecte-de-donnees-personnelles

6 La tenue du registre de traitement, comment faire ?

Un registre par type de traitement

Il ne s'agit pas de faire un registre par patient que vous recevez ou pour chaque salarié que vous employez.

Au sein de votre cabinet, les traitements que vous pouvez avoir sont les données relatives aux patients et éventuellement les données relatives au personnel employé.

Les traitements doivent être répertoriés dans un registre des activités de traitement.
Ce registre vous permet de recenser de façon précise les traitements de données personnelles que vous mettez en œuvre.

Ce registre peut être sous forme informatique.
Afin de vous aider dans la constitution de ce registre de traitement, le service juridique de la Fédération nationale des orthophonistes a complété un modèle qui pourra vous servir pour éditer votre propre registre.

Vous pouvez retrouver sur le site de la Fédération nationale des orthophonistes ce modèle pré-rempli ainsi que le modèle vierge mis à disposition par la CNIL. (www.fno.fr/exercice-professionnel/lexercice-liberal/divers)

APERÇU DU MODÈLE PRÉ-REMPLI :

RGPD : modèle liste de traitement

Page 1 obligatoire du registre de traitement

Identification du traitement				Acteurs	Finalité du traitement	Transferts hors UE ?	Données sensibles ?
Nom / sigle	N° / REF	Date de création	Dernière mise à jour	Responsable du traitement	Finalité principale	Oui /non	Oui/non
Marguerite FLOIRY orthophoniste	001	12/03/2018	12 mars 2018	Marguerite FLOIRY orthophoniste	tenue d'un dossier patient	NON	OUI
Marguerite FLOIRY orthophoniste	002	12/03/2018	12 mars 2018	Marguerite FLOIRY orthophoniste	tenue du dossier d'un salarié	NON	NON

MODELE

pour vous aider à compléter votre registre de traitement

Vous pouvez télécharger un registre "vierge" sur le site de la CNIL (outils pour vous aider - modèle de registre européen à télécharger)
https://www.cnil.fr/fr/cartographier-vos-traitements-de-donnees-personnelles

Modèle pour dossiers patients

Page 2 obligatoire du registre de traitement.

Fiche de registre	ref-001
Description du traitement	
Nom / sigle	Marguerite FLOIRY orthophoniste
N° / REF	ref-001
Date de création	12/03/2018
Mise à jour	12 mars 2018

Acteurs	Nom	Adresse	CP	Ville	Pays	Tel
Responsable du traitement	Marguerite FLOIRY orthophoniste	21 rue du Général Leclerc	75020	Paris	France	01.02.03.04.05
Délégué à la protection des données	Ø					
Représentant	Ø					
Responsable(s) conjoint(s)	Ø					

Finalité(s) du traitement effectué	
Finalité principale	Tenue d'un dossier patient
Sous-finalité 1	Recenser les données admnistratives
Sous-finalité 2	Prise en charge/bilan
Sous-finalité 3	facturation
Sous-finalité 4	
Sous-finalité 5	

Mesures de sécurité	
Mesures de sécurité techniques	antivirus /session verouillée par un mot de passe
Mesures de sécurité organisationnelles	Ø

Catégories de données personnelles concernées	Description	Délai d'effacement
Etat civil, identité, données d'identification, images...	nom, prénom, date de naissance, adresse postale, adresse mail, numéro de téléphone	Durée de conservation d'un dossier : 30 ans
Vie personnelle (habitudes de vie, situation familiale, etc.)	situation familiale, matrimoniale, fratrie	Durée de conservation d'un dossier : 30 ans
Informations d'ordre économique et financier (revenus, situation financière,	CMU/AME/CMU-C	Durée de conservation d'un dossier : 30 ans
Données de connexion (adress IP, logs, etc.)	Ø	
Données de localisation (déplacements, données GPS, GSM, etc.)	Ø	

Données sensibles	Description	Délai d'effacement
Données révèlant l'origine raciale ou ethnique	Ø	
Données révèlant les opinions politiques	Ø	
Données révèlant les convictions religieuses ou philosophiques	Ø	
Données révèlant l'appartenance syndicale	Ø	
Données génétiques	Ø	
Données biométriques aux fins d'identifier une personne physique de manière unique	Ø	
Données concernant la santé	Données contenues dans les bilans, dans le suivi de la prise en charge, dans le dossier médical de la carte vitale	Durée de conservation d'un dossier : 30 ans
Données concernant la vie sexuelle ou l'orientation sexuelle	Ø	
Données relatives à des condamnations pénales ou infractions	Ø	
Numéro d'identification national unique (NIR pour la France)	Numéro de sécurité sociale / numéro de mutuelle	Durée de conservation d'un dossier : 30 ans

Catégories de personnes concernées	Description
Catégorie de personnes 1	patients
Catégorie de personnes 2	assurés sociaux

Destinataires	Description	Type de destinataire	
Destinataire 1	Compte-rendu bilan/dossier	Autre (Préciser)	patients/assurés sociaux
Destinataire 2	Compte-rendu bilan	Autre (Préciser)	tout professionnel de santé amené à prendre en charge le patient (partage d'informations)
Destinataire 3	facturation	Partenaires institutionnels ou commerciaux	caisses/mutuelles
Destinataire 4			

Tranferts hors UE	Destinataire	Pays	Type de Garanties		Lien vers le doc
Organisme destinataire 1	Ø				
Organisme destinataire 2	Ø				
Organisme destinataire 3	Ø				

Si vous ne traitez que des données relatives aux patients, vous ferez uniquement un registre de traitement des données référencé 001 pour la tenue d'un dossier patient.

Modèle pour vos salariés

Page 3 du registre de traitement.

Fiche de registre						ref-002
Description du traitement						
Nom / sigle	Marguerite FLOIRY orthophoniste					
N° / REF	ref-002					
Date de création	12/03/2018					
Mise à jour	12 mars 2018					
Acteurs	Nom	Adresse	CP	Ville	Pays	Tel
Responsable du traitement	Marguerite FLOIRY orthophoniste	21 rue du Général Leclerc	75020	Paris	France	01.02.03.04.05
Délégué à la protection des données	Ø					
Représentant	Ø					
Responsable(s) conjoint(s)	Ø					
Finalité(s) du traitement effectué						
Finalité principale	Dossier personnel employé					
Sous-finalité 1	Recenser les données admnistratives					
Sous-finalité 2	bulletin de paie					
Sous finalité 3						
Sous-finalité 4						
Sous-finalité 5						
Mesures de sécurité						
Mesures de sécurité techniques	antivirus /session verouillée par un mot de passe					
Mesures de sécurité organisationnelles	Ø					
Catégories de données personnelles concernées	Description			Délai d'effacement		
Etat civil, identité, données d'identification, images...	nom, prénom, date de naissance, adresse postale, adresse mail, numéro de téléphone			Temps de présence comme employé		
Vie personnelle (habitudes de vie, situation familiale, etc.)	situation familiale, matrimoniale			Temps de présence comme employé		
Informations d'ordre économique et financier (revenus, situation	revenus			5 ans après le départ du salarié pour les bulletins de paie		
Données de connexion (adress IP, logs, etc.)	Ø					
Données de localisation (déplacements, données GPS, GSM,	Ø					
Données sensibles	Description			Délai d'effacement		
Données révèlant l'origine raciale ou ethnique	Ø					
Données révèlant les opinions politiques	Ø					
Données révèlant les convictions religieuses ou philosophiques	Ø					
Données révèlant l'appartenance syndicale	Ø					
Données génétiques	Ø					
Données biométriques aux fins d'identifier une personne physique	Ø					
Données concernant la santé	Ø					
Données concernant la vie sexuelle ou l'orientation sexuelle	Ø					
Données relatives à des condamnations pénales ou	Ø					
Numéro d'identification national unique (NIR pour la France)	Numéro de sécurité sociale			5 ans après le départ du salarié pour les bulletins de paie		
Catégories de personnes concernées	Description					
Catégorie de personnes 1	Employés					
Catégorie de personnes 2						
Destinataires	Description	Type de destinataire				
Destinataire 1	données administratives	Partenaires institutionnels ou commerciaux				
Destinataire 2	paie	Partenaires institutionnels ou commerciaux				
Destinataire 3						
Destinataire 4						
Tranferts hors UE	Destinataire	Pays	Type de Garanties		Lien vers le doc	
Organisme destinataire 1	Ø					
Organisme destinataire 2	Ø					
Organisme destinataire 3	Ø					

Si vous avez du personnel employé (personnel de ménage, secrétariat), vous devrez faire un registre de traitement des données référencé 002 pour la tenue du dossier salarié.

Le registre est à mettre à jour (attention à bien indiquer la date de mise à jour à l'emplacement réservé à cet effet) si vous êtes amené à modifier le type de données que vous traitez.
Par exemple, vous n'aviez pas de salariés et vous décidez d'embaucher. Il faudra mettre à jour votre registre et créer la page 3 ci-contre.

Si vous exercez à plusieurs au sein de votre cabinet avec un logiciel multi-praticien, si vous exercez au sein d'une MSP, ESP, SISA, etc ... :
Chaque professionnel doit faire son propre registre de traitement.

7 Je dois me mettre en conformité, dois-je passer par un prestataire extérieur ?

Le RGPD doit être appliqué à compter du 25 mai 2018 mais attention ne vous précipitez pas en faisant appel à n'importe quel prestataire.

Tout comme pour la mise aux normes accessibilité des locaux, des sociétés peu scrupuleuses peuvent se présenter à vous afin de vous faire peur et vous inciter à faire appel à elles pour constituer votre registre de traitement.

ATTENTION : Mise en garde sur les risques de démarchage agressif autour du RGPD.

Le site de la CNIL est très complet et ils ont mis un numéro de téléphone dédié aux professionnels de la santé. **En cas de doute, n'hésitez pas, appelez la CNIL.**

8 Quelle sanction ?

Le RGPD prévoit des sanctions particulièrement élevées en cas d'infraction :4 % du chiffre d'affaires annuel de l'exercice précédent.
Ex : pour un CA moyen de 50.000 € l'amende serait de 2.000 €.

CNIL Santé

Tous les lundis de 10h à 12h et jeudis de 14h30 à 16h30.
Par téléphone au 01 53 73 22 22.
www.cnil.fr/professionnel

9 Qu'est-ce que l'étude d'impact ?

Dernier point et pas des moindres, mais ne vous précipitez pas, là non plus…
Une étude d'impact est requise lorsqu'un type de traitement est « *susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques* » article 35 du RGPD.
Un cabinet d'orthophonie traite des données sensibles relatives à la santé donc le RGPD prévoit que le responsable de traitement doit réaliser une étude d'impact.

Délai de 3 ans pour l'étude d'impact : si vous avez fait une déclaration simplifiée précédemment.

En effet, si vous avez précédemment réalisé auprès de la CNIL une déclaration simplifiée, vous disposez d'un délai de 3 ans pour faire cette étude d'impact sauf si vous ajoutez un nouveau traitement de données et vous mettez à jour votre registre de traitement (par exemple vous embauchez un salarié).

L'étude d'impact permet d'obtenir une bonne connaissance des mesures contribuant à la sécurité des données personnelles sensibles et d'obtenir une bonne compréhension des causes et conséquences des risques (par exemple : quelles conséquences sur la vie privée si les données de mes patients sont piratées ?).

La CNIL met à disposition un logiciel permettant de réaliser plus facilement cette étude d'impact.

www.cnil.fr/fr/outil-pia-telechargez-et-installez-le-logiciel-de-la-cnil

Cependant, la CNIL nous a informés que pour les petites structures, du type cabinet libéral, des mesures d'exception seraient éventuellement mises en place au fur et à mesure. Pour l'instant rien de sûr mais cette étude d'impact pourrait ne pas être aussi contraignante qu'elle semble l'être actuellement.

Nous ne manquerons pas de vous tenir informé de l'évolution de ce RGPD qui va petit à petit se mettre en place.