ORDRE NATIONAL
DES PÉDICURES-PODOLOGUES

Guide pratique

Le pédicure-podologue et la protection des données personnelles

MARS 2020

ORDRE NATIONAL
DES PÉDICURES-PODOLOGUES

DELSOL AVOCATS
LA QUALITÉ DE LA RELATION

Le guide pratique intitulé **« Le pédicure-podologue et la protection des données personnelles »** a été réalisé avec le concours du département Données Personnelles du Cabinet DELSOL Avocats.

Table des matières

6071647.3

I. Préambule

1. Pourquoi un guide sur la protection des données personnelles pour les pédicures-podologues ?

⇨ Introduction du RGPD et de la loi Informatique et Libertés

Le sujet de la protection des données personnelles constitue un enjeu important pour les pédicures-podologues qui doivent désormais s'assurer de la conformité de leurs traitements aux dispositions du Règlement européen sur la protection des données personnelles du 27 avril 2016 (RGPD) entré en application le 25 mai 2018, de la loi Informatique et Liberté modifiée et de son décret d'application du 29 mai 2019 (ci-après la « Réglementation applicable à la protection des données »).

Ces textes constituent désormais le cadre juridique de la protection des données personnelles en Europe d'abord, puis en France et s'appliquent à toute personne physique ou morale quel que soit son secteur d'activité, y compris les pédicures-podologues.

Au titre du principe de responsabilisation des acteurs, vous devez être en mesure de démontrer à tout moment votre conformité aux principes de protection des données personnelles en documentant toutes les démarches entreprises à cet effet : mise en place d'un registre de vos traitements de données personnelles, information délivrée aux patients et à votre personnel, actions menées pour garantir la sécurité de vos données, etc.

Le présent guide pratique a pour objectif d'orienter et d'aider les pédicures-podologues inscrits au tableau de l'Ordre dans la mise en œuvre de leurs obligations.

⇨ Rôle du CNOPP

En tant que défenseur de la légalité et de la moralité professionnelle des pédicures-podologues[1], le Conseil national de l'ordre des pédicures-podologues (CNOPP) vous accompagne dans le respect de vos obligations légales parmi lesquelles figure le respect de la Réglementation applicable sur la protection des données personnelles.

A ce titre, le CNOPP informe et sensibilise les pédicures-podologues sur l'application des principes de la protection des données personnelles et ses impacts sur les traitements mis en œuvre à travers ce guide.

D'autre part, le CNOPP particulièrement soucieux du respect des principes de protection de données personnelles a désigné un délégué à la protection des données (DPD) ou « Data Privacy Officer » en la personne de Monsieur Bernard BARBOTTIN.

A ce titre, ses missions sont en particulier les suivantes :

- accompagner le CNOPP dans la mise en conformité de ses traitements
- informer et conseiller le CNOPP sur ses obligations en matière de protection des données
- sensibiliser les conseillers et collaborateurs de l'Ordre : réunions et formations
- auditer régulièrement le respect des principes de protection de données personnelles
- répondre à toute demande relative à la protection des données personnelles

[1] Article L. 4322-7 du code de la santé publique

Le DPO peut être joint par email à l'adresse suivante dpo@cnopp.fr et par téléphone au numéro suivant 06.43.80.56.10 pour toute question relative à l'exercice des droits qui vous sont conférés au titre du RGPD sur les données à caractère personnel vous concernant et détenues par l'Ordre, ou par courrier à l'adresse suivante :

M. Bernard BARBOTTIN
Délégué à la protection des données - DPO
Ordre national des pédicures-podologues
116 rue de la Convention
75015 Paris

Par ce guide, le CNOPP souhaite accompagner les pédicures-podologues dans leur mise en conformité avec la Réglementation relative à la protection des données personnelles et attirer leur vigilance sur la présence d'arnaques de sociétés proposant des services de mise en conformité.

Attention aux arnaques au RGPD !

La Commission nationale Informatique et Libertés (CNIL) dénonce les démarchages trompeurs qui lui ont été signalés, notamment les organismes qui proposent un formulaire « Déclaration normale RGPD » reproduisant frauduleusement le logo de la CNIL ou encore ceux qui adressent des courriers « Mise en conformité – dernier rappel » avec le logo usurpé de la CNIL ou des fax « RGPD – Mise en conformité » invitant à appeler un numéro de téléphone pour ensuite facturer la fausse mise en conformité au RGPD.

Vous devez donc rester vigilants face à de telles sollicitations et en cas de doute sur la probité d'un démarchage, l'Ordre vous invite à prendre contact au plus tôt avec lui, le DPO ou la CNIL.

2. Quelques définitions pour comprendre la protection des données personnelles

⇨ Qu'est-ce qu'une **donnée personnelle** ?

Une donnée personnelle désigne toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres. Ainsi, les nom, prénom, date de naissance, numéro de téléphone, numéro de sécurité sociale des patients que vous suivez dans le cadre de votre activité professionnelle sont des données personnelles.

⇨ Qu'est-ce qu'une **donnée personnelle de santé** ?

Une donnée personnelle de santé se rapporte à l'état de santé d'une personne concernée qui révèle des informations sur son état de santé physique ou mentale passé, présent ou futur quelle que soit la source de production de la donnée (un professionnel de santé ou un dispositif médical par exemple).

Par exemple, sont considérées comme des données de santé, toutes informations médicales (une donnée clinique ou thérapeutique, physiologique ou biologique) relatives à un patient dans le cadre de sa prise en charge qui vous permettent d'effectuer des actes médicaux[2] (traitement des verrues plantaires, des ongles incarnés, soins d'hygiène du pied, prescription, confection et application des prothèses).

[2] Article R.4322-1 du code de la santé publique

La prise de Rendez-vous comporte des données personnelles, en particulier les données d'identification (nom, prénom) et les données relatives à la santé traitement envisagé, antécédents, ...).

En tout état de cause, les données de santé sont des catégories particulières de données qui revêtent un caractère sensible et qui doivent être particulièrement protégées.

⇨ Qu'est-ce qu'un **traitement de données personnelles** ?

Un traitement désigne toute opération ou tout ensemble d'opérations portant sur ce type de données, quel que soit le procédé ou support utilisé (papier, numérique...), et notamment la collecte, l'enregistrement, l'utilisation de toute donnée personnelle. Par exemple, la gestion du dossier médical de votre patient, la gestion de personnel, la gestion des relations avec les fournisseurs.

⇨ Qu'est-ce qu'un **responsable de traitement** ?

Le responsable de traitement désigne la personne, l'autorité publique, le service ou l'organisme qui détermine les finalités et les moyens du traitement, sauf désignation expresse par un texte de nature législative ou règlementaire.

En conséquence, le pédicure-podologue exerçant son activité en libéral est responsable des traitements informatiques ou papier qu'il met en œuvre et gère.

A l'inverse, un pédicure-podologue qui exerce en qualité de salarié au sein d'un hôpital n'est pas responsable des traitements mis en œuvre par l'établissement.

⇨ Qu'est-ce qu'un **sous-traitant** ?

Le sous-traitant désigne toute personne traitant des données personnelles pour le compte du responsable du traitement. Il agit sous l'autorité du responsable du traitement et sur ses instructions.

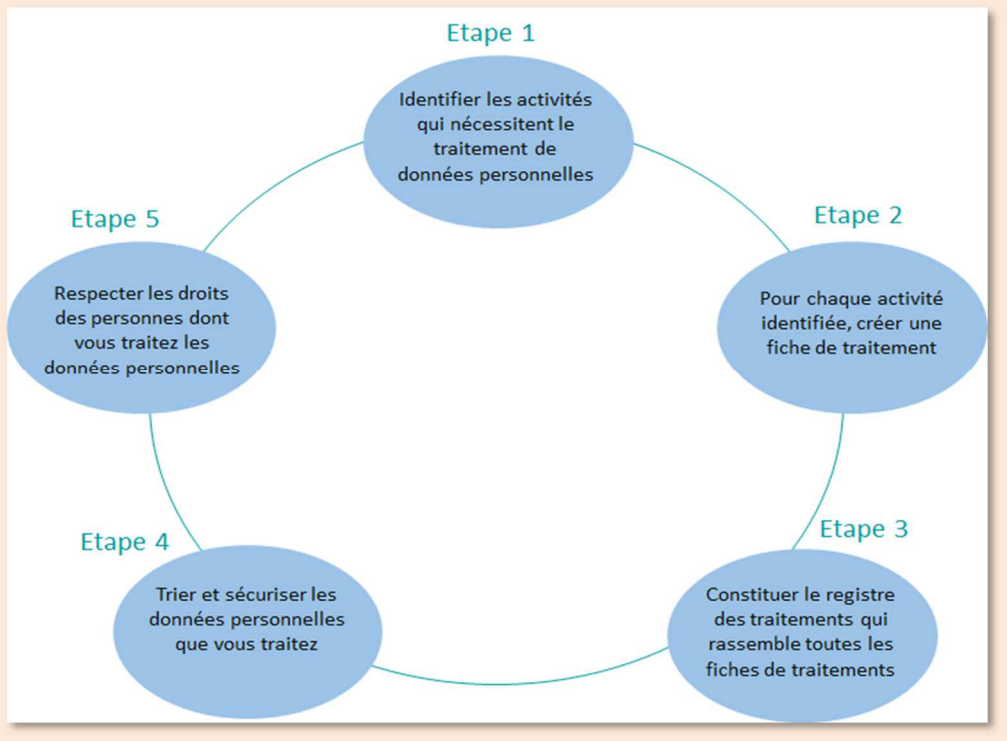
Par exemple, le prestataire informatique qui édite le logiciel métier que vous utilisez dans le cadre du suivi de vos patients est un sous-traitant. Il agit **sous votre autorité** en tant que responsable du traitement et **sur ses instructions**. Il doit présenter des garanties suffisantes en matière de sécurité et de confidentialité.

Il est important de préciser à ce stade que le responsable de traitement reste responsable de tout manquement commis par ses sous-traitants.

II. Comment passer à l'action ?

1. Quelles sont les actions à mener pour protéger les données personnelles collectées ?

⇨ Cycle des actions de conformité



⇨ Désigner un pilote

L'article 37 du RGPD prévoit que la désignation du DPO est obligatoire dans trois cas :

- pour toute autorité publique ou tout organisme public ;
- si les activités de base de l'organisme consistent en des traitements qui, du fait de leur nature, de leur portée et/ou de leurs finalités, exigent un suivi régulier et systématique à grande échelle des personnes concernées ;
- si les activités de base de l'organisme consistent en des traitements à grande échelle de données sensibles, ou de données relatives aux condamnations et infractions spéciales.

Au regard des critères posés par le RGPD, le pédicure-podologue libéral n'a pas à désigner de délégué à la protection des données (DPO).

En l'absence de désignation d'un DPO et en cas d'exercice en groupe, nous vous conseillons de désigner une personne au sein de votre personnel car le référent est important (en cas d'exercice des droits des patients du cabinet, de notification d'une violation de données, en particulier lorsqu'elle porte sur des données de santé, pour être l'interlocuteur privilégié avec la CNIL...). Cette personne sera en charge des questions relatives à la protection des données personnelles et s'assurera du respect des obligations imposées par la Réglementation sur la protection des données personnelles.

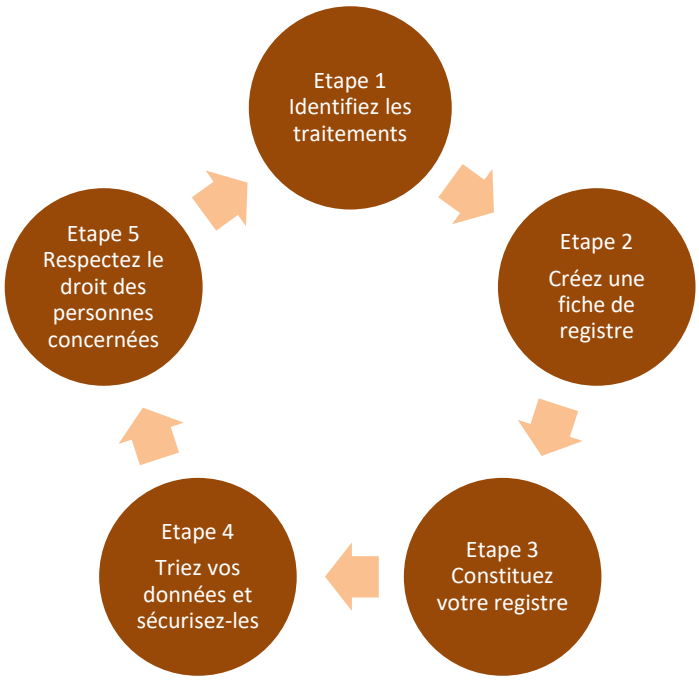
⇨ Identifier les activités et les fichiers dans lesquels sont traitées des données personnelles

Depuis l'entrée en vigueur du RGPD, vous n'êtes plus tenu d'accomplir des formalités préalables auprès de la CNIL. Néanmoins, vous devez être en mesure de démontrer à tout moment votre conformité aux principes de protection des données personnelles en documentant toutes les démarches entreprises.

A ce titre, vous devez mettre en place un registre des traitements conformément à l'article 30 du RGPD qui doit comprendre les informations suivantes.

Noms et coordonnées du responsable du traitement, de son représentant et du DPO	**Catégories de destinataires auxquels les données seront communiquées**
Finalités du traitement	Transferts de données à caractère personnel mis en œuvre
Catégories de personnes concernées	Délais prévus pour l'effacement des différentes catégories de données
Catégories de données à caractère personnel	Mesures de sécurité techniques et organisationnelles

Pour créer votre registre des traitements, il est nécessaire de respecter les étapes suivantes.



- Sa mise à jour : les bons réflexes

✓ Vérifier que les fiches de registre sont à jour (2 fois par an par exemple)
✓ S'assurer que les fiches reflètent la réalité des traitements mis en œuvre, par exemple si vous changez de prestataire qui agit en tant que sous-traitant, vous devez l'indiquer dans la fiche de registre appropriée

- ✓ Conserver une trace des modifications qui ont été faites, par exemple : en enregistrant le fichier modifié dans un nouveau document Word faisant apparaître la date d'enregistrement dans le titre : « registre des traitements version XX/XX/XXXX ».

Un modèle de fiche de registre adapté à chaque type de traitement que vous mettez en œuvre est mis à votre disposition dans ce guide.

⇨ Vérifier que vos traitements sont conformes à la Réglementation relative à la protection des données personnelles

Quand vous traitez des données personnelles, vous devez respecter les principes de protection des données suivants.

- Une finalité déterminée et légitime

Les données personnelles que vous collectez, traitez, communiquez le cas échéant et conservez, doivent être utilisées en vue d'une finalité déterminée. Il peut s'agir d'une obligation par exemple la gestion du suivi de vos patients.

Chaque finalité de traitement doit avoir un fondement qui justifie sa mise en œuvre[3]. Ainsi un traitement est licite s'il repose sur :

- ✓ le consentement de la personne concernée
- ✓ l'exécution d'un contrat
- ✓ une obligation légale à laquelle le responsable du traitement est soumis
- ✓ la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne physique
- ✓ l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement
- ✓ l'intérêt légitime du responsable de traitement

Il est souhaitable de ne retenir qu'un seul fondement par finalité de traitement.

Toute utilisation personnelle ou commerciale des données personnelles des patients est naturellement prohibée.

- Des données adéquates, pertinentes, non excessives et mises à jour

Seules les données personnelles nécessaires à votre activité doivent être traitées.

Par exemple, il n'est pas utile de collecter les données relatives à l'orientation sexuelle de vos patients pour réaliser vos actes médicaux ou encore de collecter le numéro de sécurité sociale de votre fournisseur.

- Une durée de conservation limitée

Les données personnelles doivent être conservées pour une durée déterminée. Par exemple, les données qui sont traitées pour la gestion du dossier de suivi du patient doivent être conservées pendant une durée de 20 ans à compter de la dernière consultation.

[3] Principe de licéité des traitements visé par l'article 6 du RGPD

- Une obligation de sécurité

Des mesures de sécurité doivent être mises en place afin de garantir l'intégrité et la confidentialité des données personnelles que vous traitez, en particulier celles qui sont couvertes par le secret médical et empêcher qu'elles ne soient déformées, endommagées ou communiquées à des tiers non autorisés.

Afin d'empêcher les tiers d'accéder de façon non autorisée aux données personnelles des personnes concernées, vous êtes tenus de mettre en œuvre toutes les mesures de physiques et informatiques nécessaires à la sécurité et confidentialité des données.

En tant que professionnel libéral, vous accédez aux données de vos patients en utilisant votre carte de professionnel de santé. Les personnels placés sous votre autorité doivent également disposer d'une carte d'accès ou d'un mot de passe personnel conforme aux recommandations de la CNIL[4] (12 caractères comportant des chiffres, des lettres majuscules et minuscules, des caractères spéciaux), renouvelé régulièrement.

Modèle de bonnes pratiques qui peuvent vous concerner

Bonnes pratiques	Mesures
Sensibiliser les utilisateurs	Informer et sensibiliser les personnes manipulant les données aux bonnes pratiques élémentaires de l'informatique
	Rédiger une charte informatique et lui donner une force contraignante
Authentifier les utilisateurs	Définir un identifiant unique à chaque utilisateur
	Adopter une politique de mot de passe utilisateur conforme aux recommandations de la CNIL
	Obliger l'utilisateur à changer son mot de passe après réinitialisation
	Limiter le nombre de tentative d'accès à un compte
Gérer les habilitations	Définir les profils d'habilitation
	Supprimer les permissions d'accès obsolètes
	Réaliser une revue annuelle des habilitations
Tracer les accès et gérer les incidents	Prévoir un système de journalisation
	Informer les utilisateurs de la mise en place du système de journalisation
	Protéger les équipements de journalisation et les informations journalisées
	Prévoir les procédures pour les notifications de violation de données à caractère personnel
Sécuriser les postes de travail	Prévoir une procédure de verrouillage automatique de session
	Utiliser des antivirus régulièrement mis à jour
	Installer un « pare-feu » (firewall) logiciel
	Recueillir l'accord de l'utilisateur avant toute intervention sur son poste
Sécuriser l'informatique mobile	Prévoir des moyens de chiffrement des équipements mobiles
	Faire des sauvegardes ou des synchronisations régulières des données
	Exiger un secret pour le déverrouillage des smartphones
Protéger le réseau	Limiter les flux réseau au strict nécessaire
	Sécuriser les accès distants des appareils informatiques nomades par VPN

[4] https://www.cnil.fr/fr/authentification-par-mot-de-passe-les-mesures-de-securite-elementaires

informatique interne	Mettre en œuvre le protocole WPA2 ou WPA2-PSK pour les réseaux Wi-Fi
Sécuriser les serveurs	Limiter l'accès aux outils et interfaces d'administration aux seules personnes habilitées
	Installer sans délai les mises à jour critiques
	Assurer une disponibilité des données
Sécuriser les sites web	Utiliser le protocole TLS et vérifiez sa mise en œuvre
	Vérifier qu'aucun mot de passe ou identifiant ne passe dans les url
	Contrôler que les entrées des utilisateurs correspondent à ce qui est attendu
	Mettre un bandeau de consentement pour les cookies non nécessaires au service
Sauvegarder et prévoir la continuité d'activité	Effectuer des sauvegardes régulières
	Stocker les supports de sauvegarde dans un endroit sûr
	Prévoir des moyens de sécurité pour le convoyage des sauvegardes
	Prévoir et tester régulièrement la continuité d'activité
Archiver de manière sécurisée	Mettre en œuvre des modalités d'accès spécifiques aux données archivées
	Détruire les archives obsolètes de manière sécurisée
Encadrer la maintenance et la destruction des données	Enregistrer les interventions de maintenance dans une main courante
	Encadrer par un responsable de l'organisme les interventions par des tiers
	Effacer les données de tout matériel avant sa mise au rebut
Gérer la sous-traitance	Prévoir une clause spécifique dans les contrats des sous-traitants
	Prévoir les conditions de restitution et de destruction des données
	Vous assurer de l'effectivité des garanties prévues (audits de sécurité, visites, etc.)
Sécuriser les échanges avec d'autres organismes	Chiffrer les données avant leur envoi
	Vérifier qu'il s'agit du bon destinataire
	Transmettre le secret lors d'un envoi distinct et via un canal différent
Protéger les locaux	Restreindre les accès aux locaux au moyen de portes verrouillées
	Installer des alarmes anti-intrusion et les vérifier périodiquement
Encadrer les développements informatiques	Proposer des paramètres respectueux de la vie privée aux utilisateurs finaux
	Éviter les zones de commentaires ou les encadrer strictement
	Tester sur des données fictives ou anonymisées
Utiliser les fonctions cryptographiques	Utiliser des algorithmes, des logiciels et des bibliothèques reconnues
	Conserver les secrets et les clés cryptographiques de manière sécurisée

Pour plus d'informations, vous pouvez consulter le guide de la CNIL sur « La sécurité des données personnelles » ainsi que le guide de l'ANSSI « Guide d'hygiène informatique ».

- Le respect des droits de la personne

Vous devez informer les personnes concernées par les données que vous collectez et traitez (par exemple les patients ou votre personnel) de l'existence des traitements mis en place et des modalités d'exercice de leurs droits : droit d'accès, de rectification, d'opposition, de portabilité, d'effacement ou de limitation du traitement de leurs données personnelles.

Avant de transmettre des données personnelles, vous devez vous assurer que le destinataire est habilité à recevoir lesdites données.

Vous engagez votre responsabilité si vous transmettez des données personnelles à des personnes qui n'ont pas à en connaître.

D'autre part, le fait de transmettre des données pour une finalité autre que celle pour laquelle les données ont été collectées correspond à un nouveau traitement de données personnelles qui devra dès lors respecter les principes de protection des données.

⇨ Informer les personnes dont vous collectez ou conservez des données personnelles et respecter leurs droits

Conformément à l'article 13 du RGPD, plusieurs informations doivent être communiquées au moment de la collecte aux personnes concernées par le traitement mis en place.

Cela signifie en pratique que l'information doit comporter les éléments suivants[5] :

- le nom de votre cabinet agissant en qualité de responsable de traitement et ses coordonnées ;
- les finalités et le fondement du traitement (consentement, exécution d'un contrat, obligation légale, etc.) ;
- les destinataires des données
  - en interne : il s'agit des personnes habilitées en interne qui reçoivent les données collectées dans le cadre du traitement visé : par exemple les professionnels de santé qui partagent le même cabinet et qui interviennent dans la prise en charge du patient ;
  - en externe : il s'agit des organismes de sécurité sociale et de l'assurance maladie dans le cadre de la prise en charge des patients ou encore les sous-traitants qui traitent les données pour votre compte (licence d'utilisation et maintenance informatique de l'application utilisée dans le cadre du suivi des patients, établissement des bulletins de paie du personnel, gestion de la comptabilité par un cabinet d'expert-comptable) ;
- la durée de conservation ;
- les droits de la personne : accès, rectification, à certaines conditions effacement, limitation, opposition, possibilité de saisir, le cas échéant, la CNIL d'une réclamation.

Un modèle de mention d'information adapté à chaque type de traitement que vous mettez en œuvre est mis à votre disposition dans chaque fiche présentée au sein du guide.

[5] Article 13 du RGPD.

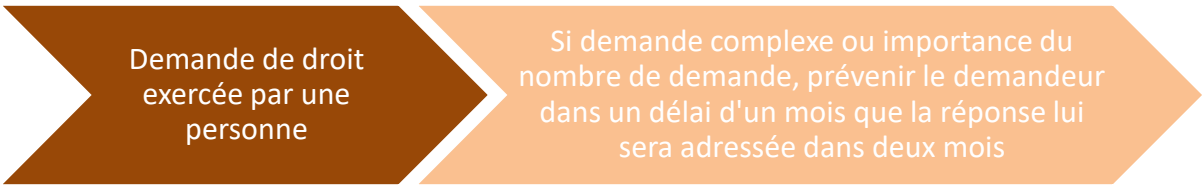
- Comment répondre à une personne exerçant ses droits ?

Chaque demande d'exercice d'un des droits précités doit être examinée dans les meilleurs délais, soit **dans un délai d'un mois à compter de la réception de la demande, à l'exception des données relatives au suivi des patients pour lesquels le délai de réponse ne doit pas excéder huit jours[6] à compter de la réception de la demande**.

Ce délai **peut être prolongé de deux mois**, au regard de la complexité et du nombre de demandes. Le responsable du traitement informe la personne concernée de cette prolongation et des motifs du report dans un délai d'un mois à compter de la réception de la demande.

Demande « simple »

Demande complexe



⇨ Analyser et gérer les risques

Le respect de la réglementation relative à la protection des données personnelles suppose d'analyser et d'anticiper les risques pour les droits et libertés des personnes concernées.

A cette fin, une analyse d'impact sur la vie privée (AIPD) doit être élaborée dans l'hypothèse où un traitement de données personnelles est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes concernées.

L'analyse d'impact sur la vie privée sur la protection des données vise ainsi à :

- **déterminer les risques** pour les droits et libertés des personnes concernées que présente un traitement de données,
- **définir les actions à mettre en place** pour faire diminuer ces risques et protéger les données.

Cette analyse d'impact implique la réalisation de trois phases successives :

1) une description détaillée du traitement mis en œuvre, comprenant tant les aspects techniques qu'opérationnels,

2) l'évaluation, de nature plus juridique, de la nécessité et de la proportionnalité concernant les principes et droits fondamentaux (finalité, données et durées de conservation, information et droits des personnes, etc.) qui sont fixés par la loi et doivent être respectés, quels que soient les risques ;

[6] Art. L.1111-7 du code de la santé publique.

3) l'étude, de nature plus technique, des risques sur la sécurité des données (confidentialité, intégrité et disponibilité) ainsi que leurs impacts potentiels sur la vie privée, qui permet de déterminer les mesures techniques et organisationnelles nécessaires pour protéger les données.

Dans le cadre de votre activité de pédicure-podologue, vous n'êtes pas tenu de réaliser une analyse d'impact. En effet, la CNIL a expressément listé parmi les traitements pour lesquels il n'est pas nécessaire de réaliser une analyse d'impact, les « *Traitements de données de santé nécessaires à la prise en charge d'un patient par un professionnel de santé exerçant à titre individuel au sein d'un cabinet* ».

⇨ Notifier les violations de données personnelles

Une violation de données personnelles désigne une violation de la sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de données personnelles transmises, conservées ou traitées d'une autre manière, ou l'accès non autorisé à de telles données.

Constituent une violation de données personnelles les exemples suivants :

- ✓ Une perte de données personnelles lors de la perte ou du vol d'une clé USB (dont l'usage est d'ailleurs déconseillé) contenant une copie de la base de données patients de votre cabinet,
- ✓ Une suppression accidentelle des données de santé de vos patients,
- ✓ Une introduction malveillante sur les bases de données de votre cabinet,
- ✓ Un accès non autorisé à vos bases de données.

Il se peut que vous constatiez une violation de données personnelles directement ou indirectement (par le biais d'un sous-traitant).

A ce titre, vous devez apprécier au cas par cas si :

- ➢ **Si la violation n'entraîne pas de risque** pour les droits et libertés des personnes concernées, par exemple l'accès par erreur d'une personne non habilitée aux données personnelles collectées dans le cadre de la gestion des prestataires, le responsable de traitement

  - doit documenter, en interne sous forme d'un registre (tel que vu précédemment), la violation qui vient de se produire ;
  - ne doit pas notifier cette violation à la CNIL et aux personnes concernées.

- ➢ **Si la violation entraîne un risque pour les droits et libertés des personnes concernées,** par exemple si une personne transfert les données personnelles d'un de ses salariés à un destinataire qui n'est pas habilité à les recevoir, le responsable de traitement

  - doit documenter, en interne sous forme d'un registre, la violation qui vient de se produire ;
  - doit notifier cette violation à la CNIL.

- ➢ **Si la violation entraîne un risque élevé** pour les droits et libertés des personnes concernées, par exemple si les données de santé de vos patients collectées dans le cadre de leur suivi sont publiées sur internet.

Le responsable de traitement

- doit documenter, en interne sous forme d'un registre, la violation qui vient de se produire ;
- doit notifier cette violation à la CNIL.
- doit communiquer la violation aux personnes concernées**.**

Conformément à l'article 30 du RGPD, le responsable de traitement doit **notifier la violation de données personnelles auprès de la CNIL dans un délai de 72 heures après en avoir pris connaissance.** Il est donc important d'être réactif en cas de survenance d'un incident pour déterminer s'il s'agit d'une violation de données ou non et de la notifier à la CNIL dans le délai imparti.

La notification à la CNIL s'effectue par le biais d'un téléservice sécurisé dédié accessible sur le site Internet de la CNIL.

En tout état de cause, vous devez documenter toutes violations de données personnelles que celles-ci nécessitent ou non une notification à la CNIL et/ou aux personnes concernées.

Cette documentation prend la forme d'un registre des violations qui doit comprendre les éléments suivants.

- ✓ La nature de la violation
- ✓ Les catégories et le nombre approximatif des personnes concernées
- ✓ Les catégories et le nombre approximatif de fichiers concernés
- ✓ Les conséquences probables de la violation
- ✓ Les mesures prises pour remédier à la violation et, le cas échéant, pour limiter les conséquences négatives de la violation
- ✓ Le cas échéant, la justification de l'absence de notification auprès de la CNIL ou d'information aux personnes concernées.

En pratique vous pouvez vous aider du formulaire de notification mis en ligne par la CNIL. Il vous servira de canevas pour la documentation interne et peut constituer un outil unique de gestion de la conformité en matière de violations de données personnelles.

2. Pouvez-vous être sanctionné ?

Si vous ne respectez pas vos obligations, vous pouvez faire l'objet d'une sanction administrative de la Commission Nationale Informatique et Libertés (CNIL), voire d'une sanction pénale.

La CNIL peut prononcer, en fonction de la gravité du non-respect des obligations visées par le RGPD et après instruction par ses services et après une procédure contradictoire, des amendes administratives pouvant s'élever jusqu'à 10 000 000 ou 20 000 000 d'euros[7].

Les sanctions pénales maximales pouvant être prononcées, sont, pour une personne physique, de 5 ans d'emprisonnement et de 300 000 euros d'amende[8] et, pour une personne morale, de 1,5 millions d'euros d'amende[9].

Il est donc impératif de vous mettre en conformité avec la réglementation et de documenter cette conformité (registre des activités de traitement, information des personnes concernées, engagements de confidentialité du personnel, etc.).

[7] Article 83 du RGPD
[8] Article 226-16 et suivants du code pénal
[9] Article 131-38 et article 226-24 du code pénal

Si la CNIL 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.

En respectant les recommandations formulées dans le présent guide, vous serez en mesure de démontrer votre démarche de mise en conformité au RGPD et de manière plus générale, du respect de la Réglementation applicable à la protection des données.

III. Fiches pratiques

FICHE N°1 - Quelles sont vos obligations à l'égard de vos patients ?

Check-list des bonnes pratiques à respecter :

- ⇨ Limiter les informations collectées au nécessaire pour l'accomplissement de vos actes médicaux réalisés en tant que pédicure-podologue dans le cadre du suivi de vos patients
- ⇨ Tenue d'un registre des traitements mis à jour régulièrement
- ⇨ Ne pas conserver les informations des patients au-delà des durées de conservations convenues
- ⇨ Mise en place des mesures de sécurité techniques et organisationnelles pour protéger les données des patients
- ⇨ Informer les patients sur leurs droits et leurs modalités d'exercice sur leurs données personnelles

1) Dans quelles situations pouvez-vous collecter les données personnelles de vos patients ?

Dans le cadre de l'exercice de votre profession, vous êtes amenés à collecter les données personnelles de vos patients afin d'**assurer leur suivi et réaliser des actes** conformément aux articles L4322-1 et R4322-1 du code de la santé publique. Ce traitement est donc fondé sur une obligation légale telle que prévue par les dispositions du code précité.

De manière générale, ce traitement sert à votre activité de dispensation des actes, de diagnostic et de prescription pour la réalisation de prothèses.

2) Quelles sont les données de vos patients que vous pouvez collecter ?

Dans le cadre du suivi de vos patients, vous êtes amené à traiter plusieurs catégories de données personnelles telles que décrites dans le tableau ci-après.

Catégories de données personnelles	Données personnelles collectées
Données d'identification	Nom, prénom, date de naissance, sexe, adresse, numéro de téléphone, numéro de sécurité sociale
Données relatives à la santé	Dossier du patient qui peut comprendre les prescriptions d'autres professionnels de santé, à commencer par celles du médecin traitant, ainsi que les traitements en cours.

Toute information qui serait sans lien avec votre activité de pédicure-podologue et qui ne serait pas nécessaire à la réalisation de celle-ci ne peuvent être collectées. Tel est le cas des données portant par exemple sur leur religion.

En effet, ces données sensibles ne rentrent pas dans le champ d'application du traitement relatif au suivi de vos patients tel que décrit par les articles L4322-1 et R4322-1 du code de la santé publique.

Dès lors, il convient de s'en assurer au sein des applications utilisées dans le cadre de votre activité.

3) Pendant combien de temps conserver les données de vos patients ?

Les données personnelles doivent être conservées pour une durée déterminée en fonction de la finalité ayant conduit à la collecte de celles-ci.

Dans le cadre de votre traitement portant sur le suivi de vos patients, vous pouvez conserver leurs données pendant[10] :

- 20 ans à compter de la date de sa dernière consultation ;
- si le patient est mineur et que ce délai de 20 ans expire avant son 28ème anniversaire, la conservation des informations le concernant doit être prolongée jusqu'à cette date ;
- dans tous les cas, si le patient décède moins de 10 ans après sa dernière consultation, les informations le concernant doivent être conservées pendant 10 ans à compter de la date du décès ;
- en cas d'action tendant à mettre en cause la responsabilité du médecin, il convient de suspendre ces délais de conservation.

Les doubles des feuilles de soins doivent être conservés 3 mois.

Au terme de ces durées de conservation, les données devront être supprimées.

4) Comment sécuriser les données de vos patients ?

- Liste des mesures de sécurité pouvant être mises en œuvre

Des mesures de sécurité doivent être mises en place afin de garantir l'intégrité et la confidentialité des données personnelles que vous traitez. En effet, la protection des données personnelles implique de mettre en place des *« mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque*[11].»

En particulier, dans la mesure où vous traitez des données de santé, vous devez respecter les mesures prévues par les référentiels de sécurité et d'interopérabilité des données de santé[12].

A ce titre, il convient d'ajouter de mettre en place les mesures suivantes :

- des mesures de traçabilité : journalisation des accès des utilisateurs sur 6 mois avec conservation des identifiants, date et heure de connexion, durée de connexion et documents ou dossiers consultés ;
- chiffrement des données : le logiciel utilisé pour le suivi des patients chiffre les données contenues ;
- contrôle des sous-traitants : vous devez vous assurer que vos contrats conclus avec vos sous-traitants, en particulier vos prestataires informatiques, qu'ils ont été mis à jour conformément aux dispositions de l'article 28 du RGPD.

Prévoir le cas des cabinets où plusieurs professionnels exercent. Bon usage pour protéger l'accès aux données : protection des données sur ordinateur avec mot de passe, conservation des dossiers papiers dans un placard fermé à clef, etc.

[10] Article R. 1112-7 du code de la santé publique
[11] Article 24 du RGPD
[12] Article L.1110-4-1 du code de la santé publique

Préciser le cas de la communication aux ayants-droits ? *« permettre de connaître les causes de la mort, de défendre la mémoire du défunt ou de faire valoir leurs droits, sauf volonté contraire exprimée par la personne avant son décès »* (L.1110-4 CSP)

Pour plus d'informations sur les mesures de sécurité à mettre en place, vous pouvez consulter le guide publié par la CNIL à partir du lien suivant :
https://www.cnil.fr/sites/default/files/atoms/files/cnil_guide_securite_personnelle.pdf

- Est-il obligatoire de communiquer par messagerie sécurisée ?

L'échange d'informations relatives à la santé du patient est couvert par le secret professionnel. Lorsque cet échange s'opère par le biais d'une messagerie, il est recommandé d'utiliser une messagerie sécurisée afin de préserver la sécurité et la confidentialité des informations transmises.

Pour les professionnels de santé exerçant en libéral, la Politique générale de Sécurité des systèmes d'informations (PGSSI-S) recommande l'utilisation d'une messagerie sécurisée de santé.

L'Agence du numérique en santé (ANS, ex-ASIP Santé) a développé la MSSanté (messagerie sécurisée de santé). Désormais l'ASN et les Ordres de santé proposent d'utiliser la **messagerie « MAILIZ »** grâce à laquelle les professionnels de santé peuvent échanger des données de manière dématérialisée en toute sécurité.

Le CNOPP recommande l'utilisation de la messagerie sécurisée afin de garantir le secret professionnel, la protection des données des patients et le respect du cadre légal dans les échanges entre professionnels de santé.

Pour plus d'information consulter la page « Pratique du bulletin REPERES N°39 (Avril 2018) ou la rubrique « Sécuriser son exercice » : https://www.onpp.fr/exercice/la-profession/securiser-son-exercice/communiquer-via-messagerie-securisee.html

- Dois-je réaliser une analyse d'impact ?

L'Analyse d'impact relative à la protection des données (AIPD) est un outil qui permet de construire un traitement conforme au RGPD et respectueux de la vie privée, lorsqu'un traitement de données personnelles est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes.

La CNIL a expressément listé parmi les traitements pour lesquels il n'est pas nécessaire de réaliser une analyse d'impact « Traitements de données de santé nécessaires à la prise en charge d'un patient par un professionnel de santé exerçant à titre individuel au sein d'un cabinet »[13].

En tant que pédicure-podologue, vous n'avez pas à réaliser une AIPD.

Vous pouvez consulter la liste sur le site de la CNIL :
https://www.cnil.fr/sites/default/files/atoms/files/liste-traitements-aipd-requise.pdf

5) Comment informer vos patients ?

- Modèles de notes d'information à l'attention des patients

Dans le cadre du suivi des patients, vous pouvez utiliser la mention d'information suivante et l'adapter à votre cas :

[13] https://www.cnil.fr/sites/default/files/atoms/files/liste-traitements-aipd-non-requise.pdf

« Vos données personnelles font l'objet d'un traitement de données personnelles mis en œuvre par votre pédicure-podologue en sa qualité de responsable de traitement, à des fins de suivi de ses patients.

Vos données personnelles peuvent être transmises à d'autres professionnels de santé, par exemple votre médecin traitant, ainsi qu'aux établissements de santé dès lors qu'ils interviennent dans votre pris en charge.

Vos données personnelles sont également transmises à votre caisse de sécurité sociale dans le cade de votre prise en charge financière.

[Dans le cas d'un logiciel hébergé par un prestataire] Votre dossier est hébergé sur les serveurs de [indiquer le nom de votre prestataire] qui dispose d'un agrément / d'une certification délivrée en application des dispositions de l'article L.1111-8 du code de la santé publique et atteste d'un haut niveau de sécurité.

Dans ce contexte, vos données ne font l'objet d'aucun transfert en dehors de l'Union européenne.

Les données sont conservées pendant la durée nécessaire à leur traitement qui peut être, le cas échéant, fixée par les textes.

Conformément au Règlement européen général sur la protection des données du 27 avril 2016 et à la loi Informatique et Libertés modifiée, vous disposez d'un droit d'accès, de rectification, d'effacement de celles-ci ou une limitation du traitement aux données personnelles vous concernant en adressant un courrier électronique à l'adresse suivante : [adresse électronique] ou par courrier postal à : [adresse postale].

Vous disposez également, si vous l'estimez nécessaire, d'introduire une réclamation auprès de la Commission nationale Informatique et Libertés (CNIL). »

Cette information peut se faire par voie d'affichage (écriteau, écran digital situé au niveau de la salle d'attente) ou par le biais d'une notice d'information remise au patient.

Si vous souhaitez obtenir plus de précisions sur les informations devant être communiquées aux patients, vous pouvez également consulter la fiche de la CNIL « Conformité RGPD : comment informer les personnes et assurer la transparence » : https://www.cnil.fr/fr/conformite-rgpd-information-des-personnes-et-transparence

6) Comment respecter les droits de vos patients sur leurs données personnelles ?

Les patients disposent de droits qu'ils peuvent exercer sur leurs données personnelles, notamment leur droit d'accès, de rectification, d'effacement ou de limitation du traitement de leurs données personnelles, et déposer une réclamation auprès de la CNIL.

Pour chaque demande d'exercice, il convient de vérifier si les conditions pour exercer le(s) droit(s) visé(s) sont bien remplies ainsi que l'identité de la personne concernée, et le cas échéant d'y répondre dans les délais.

Dans le cas d'une demande d'accès au dossier « patient », le délai est obligatoirement de 8 jours, porté à 2 mois lorsque les informations datent de plus de 5 ans.[14]

Pour plus d'informations, vous pouvez consulter les fiches thématiques de la CNIL « Les droits pour maîtriser vos données personnelles » : https://www.cnil.fr/fr/les-droits-pour-maitriser-vos-donnees-personnelles

[14] Article L. 1111-7 du CSP.
L'accès au dossier date de la Loi Kouchner n°2002-303 du 4 mars 2002. Pour information un chirurgien-dentiste a été condamné par la CNIL à 10 000€ d'amende pour défaut de communication du dossier (CNIL, formation restreinte, SAN – 2017-008, 18 mai 2017)

7) Modèle prérempli d'une fiche de registre relative au suivi de vos patients

FICHE DE REGISTRE

DU SUIVI DES PATIENTS

Date de création de la fiche	
Date de dernière mise à jour de la fiche	
Nom du logiciel ou de l'application *(si pertinent)*	**Logiciel [Nom de votre application]**

Objectifs poursuivis

[Décrivez clairement l'objet du traitement de données personnelles et ses fonctionnalités.]

Le logiciel [Nom de votre application] permet le suivi des patients. Il sert à mon activité de dispensation des actes, de diagnostic, de soins, de prescription et pour la réalisation d'orthèses.

Il permet les actions suivantes :

- la gestion du dossier de suivi du patient ;
- l'établissement, l'édition et la télétransmission des feuilles de soins et factures subrogatoires ;
- l'édition et l'envoi de courriers aux professionnels de santé ;
- la gestion des règlements.

Catégories de personnes concernées

[Listez les différents types de personnes dont vous collectez ou utilisez les données.]

- Patients
- Professionnels de santé
- Le cas échéant, famille du patient
- *[A compléter si pertinent]*

Catégories de données collectées

[Cochez et listez les différentes données traitées.]

☒ État-civil, identité, données d'identification, images (ex. nom, prénom, adresse, photographie, date et lieu de naissance, etc.)

.....

☐ Vie personnelle (ex. habitudes de vie, situation familiale, etc.)

☐ Vie professionnelle (ex. CV, situation professionnelle, scolarité, formation, distinctions, diplômes, etc.)

☐ Informations d'ordre économique et financier (ex. revenus, situation financière, données bancaires, etc.)

☐ Données de connexion (ex. adresses Ip, logs, identifiants des terminaux, identifiants de connexion, informations d'horodatage, etc.)

☐ Données de localisation (ex. déplacements, données GPS, GSM, ...)

☐ Internet (ex. cookies, traceurs, données de navigation, mesures d'audience, ...)

☐ Autres catégories de données (précisez) :

Des données sensibles sont-elles traitées ?

[*La collecte de certaines données, particulièrement sensibles, est strictement encadrée par le RGPD et requiert une vigilance particulière. Il s'agit des données révélant l'origine prétendument raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale des personnes, des données génétiques et biométriques, des données concernant la santé, la vie sexuelle ou l'orientation sexuelle des personnes, des données relatives aux condamnations pénales ou aux infractions, ainsi que du numéro d'identification national unique (NIR ou numéro de sécurité sociale).*]

☒ Oui ☐ Non

Si oui, lesquelles ? : Données de santé

Durées de conservation des catégories de données

Combien de temps conservez-vous ces informations ?

Pour la gestion du dossier de suivi du patient :

20..... ☐Jours ☐Mois ☒Ans à compter de la dernière consultation

Sauf si le patient est mineur, ses données sont conservées jusqu'à son 28ème anniversaire.

Si le patient décède moins de 10 ans après sa dernière consultation, les informations le concernant doivent être conservées pendant 10 ans à compter de la date du décès.

Pour la conservation des doubles des feuilles de soins

3..... ☐Jours ☒Mois ☐Ans

Autre durée :

..... ☐Jours ☐Mois ☐Ans

Catégories de destinataires des données

Destinataires internes

- Personnel du cabinet [à conserver si applicable]
- [*A compléter si pertinent*]

Organismes externes

- Sécurité sociale
- Professionnels de santé intervenant dans la prise en charge
- Organismes d'assurance maladie complémentaire
- [*A compléter si pertinent*]

Sous-traitants

- Éditeur de logiciel [*Nom de votre application*] s'il assure une prestation de maintenance informatique ou d'hébergement de données de santé
- [*A compléter si pertinent*]

Transferts des données hors UE

Des données personnelles sont-elles transmises hors de l'Union européenne ?

☐ Oui ☒Non

Mesures de sécurité

[Cochez et décrivez les mesures de sécurité organisationnelles et techniques prévues pour préserver la confidentialité des données. Le niveau de sécurité doit être adapté aux risques soulevés par le traitement. Les exemples suivants constituent des garanties de base à prévoir et peuvent devoir être complétés.]

☒ Contrôle d'accès des utilisateurs

Décrivez les mesures : j'accède à mon application en utilisant ma carte de professionnel de santé. Les personnels placés sous mon autorité doivent également disposer d'une carte d'accès ou d'un mot de passe personnel.

☒ Mesures de traçabilité

Précisez la nature des traces (exemple : journalisation des accès des utilisateurs), les données enregistrées (exemple : identifiant, date et heure de connexion, etc.) et leur durée de conservation :

Journalisation des accès des utilisateurs sur 6 mois avec conservation des identifiants, date et heure de connexion, durée de connexion et documents ou dossiers consultés.

☒ Mesures de protection des logiciels (antivirus, mises à jour et correctifs de sécurité, tests, etc.)

Décrivez les mesures : installation d'antivirus et de pare-feu

☒ Sauvegarde des données

Décrivez les modalités : données sauvegardées hebdomadairement sur un serveur distinct

☒ Chiffrement des données

Décrivez les mesures (exemple : site accessible en https, utilisation de TLS, etc.) : le logiciel chiffre les données contenues

☒ Contrôle des sous-traitants

Décrivez les modalités : vérification des engagements pris par le sous-traitant conformément à l'article 28 du RGPD.

☐ Autres mesures :

Information et respect des droits des personnes

Comment les personnes concernées sont informées du traitement ? Cocher la ou les cases correspondantes :

☒ Mention d'information

Précisez sur quel(s) support(s) : notice d'information affichée en salle d'attente / sur un écran digital / remise en main propre

Comment sont traitées les demandes d'exercice des droits des personnes ?

Indiquez le délai du traitement de la demande : 1 mois

Indiquez la personne chargée de répondre aux demandes :

FICHE N°2 – Quelles sont vos obligations à l'égard du personnel ?

Check-list des bonnes pratiques à respecter

- ⇨ Limiter la collecte des données à ce qui est strictement nécessaire à la gestion administrative du personnel (ex : tenue du registre unique du personnel, gestion de la paie, gestion des congés, etc.)
- ⇨ Elaborer la fiche de registre relative à la gestion administrative du personnel
- ⇨ Supprimer les données personnelles des salariés au terme des durées de conservations prédéfinies
- ⇨ Mettre en place des mesures de sécurité techniques et organisationnelles pour protéger les données personnelles de vos salariés
- ⇨ Informer vos salariés de l'existence et des modalités de mise en œuvre du traitement de leurs données et des conditions d'exercice de leurs droits.

1) Dans quel contexte pouvez-vous collecter les données personnelles de vos salariés ?

- Qui est considéré comme « collaborateur » au sein d'un cabinet ?

Dans la mesure où vous exercez en tant que libéral, vous pouvez avoir recours aux services d'un(e) ou plusieurs assistant(e), y compris lorsque vous partagez votre cabinet avec d'autres professionnels de santé.

Dans les deux cas, vous collectez ses données personnelles pour une finalité déterminée, à savoir la **gestion administrative du personnel** qui porte notamment sur les fonctionnalités suivantes :

- le recrutement ;
- l'accomplissement des formalités administratives y afférentes ;
- la mise à disposition du personnel d'outils informatiques ;
- l'organisation du travail ;
- la gestion des formations du personnel,
- la gestion des carrières,
- la tenue du registre unique du personnel[15]
- la gestion de la paie.

2) Quelles données pouvez-vous collecter ?

Dans le cadre de la gestion administrative du personnel, vous traitez plusieurs catégories de données personnelles telles que décrites dans le tableau ci-après.

[15] Obligation imposée à tout établissement où sont employés des salariés en vertu de l'article L. 1221-13 du code du travail

Catégories de données personnelles	Données personnelles collectées
Données d'identification	Nom, prénom, date de naissance, sexe, adresse, numéro de téléphone
Données relatives à la vie professionnelle	CV, situation professionnelle, formation, distinctions, diplômes, nom et, le cas échéant, les coordonnées des personnes à prévenir en cas d'urgence
Données d'ordre économique et financière	Données bancaires
Données de connexion	Identifiants

Afin d'obtenir une liste plus précise des données qui peuvent être collectées dans le cadre de la gestion de votre personnel, vous pouvez consulter le référentiel relatif aux traitements de données a caractère personnel mis en œuvre par des organismes prives ou publics aux fins de gestion du personnel publié par la CNIL.

Toute donnée personnelle qui ne serait pas en lien avec la finalité du traitement ne peut être collectée. Tel est le cas des données portant sur l'orientation sexuelle de votre personnel, la religion, ou encore les opinions politiques.

3) Pendant combien de temps conserver les données de vos collaborateurs ?

Les données personnelles doivent être conservées pour une durée déterminée le temps nécessaire à la réalisation de la finalité pour laquelle elles ont été collectées.

A ce titre, vous trouverez ci-dessous un tableau récapitulatif des différentes durées de conservation applicables aux fonctionnalités mises en œuvre dans le traitement relatif à la gestion administrative du personnel et le cas échéant, de leur fondement juridique.

Fonctionnalités concernées	Durée de conservation applicable	Fondement juridique
Registre unique du personnel	5 ans à compter de la date à laquelle le salarié a quitté le cabinet	Article R.1221-26 code du travail
Recrutement	2 ans à compter du dernier contact avec le candidat non retenu	Référentiel de la CNIL
Bulletins de paie	5 ans	Article L.3243-4 code du travail
Déclarations accidents de travail auprès de la caisse primaire d'assurance maladie	5 ans	Article D.4711-3 code du travail
Documents concernant les contrats de travail, salaires, primes, indemnités, soldes de tout compte, régime de retraite	5 ans	Article 2224 du code civil
Documents relatifs aux charges sociales et à la taxe sur les salaires	3 ans	Article L.244-3 du code de la sécurité sociale et article L.169 A du livre des procédures fiscales
Comptabilisation des horaires des salariés, des heures d'astreinte et de leur compensation	1 an	Article D.3171-16 du code du travail
Données de connexion	6 mois	Doctrine de la CNIL

Pour les autres données collectées dans le cadre de la gestion de votre personnel, la durée de conservation correspond à la durée de la période d'emploi de la personne concernée.

A partir du moment où un salarié ne travaille plus au sein de votre cabinet, vous avez la possibilité de conserver pendant une durée de 5 ans ses données personnelles contenues dans votre base de données et/ou figurant sur les documents le concernant, comme sur le registre unique du personnel et les doubles de ses bulletins de paie sur support papier.

Au terme de ce délai de 5 ans à compter du départ de la personne concernée, vous devez veiller à supprimer ses données personnelles.

4) Comment sécuriser les données de vos collaborateurs ?

- Liste des mesures de sécurité possibles

Des mesures de sécurité doivent être mises en place afin de garantir l'intégrité et la confidentialité des données personnelles que vous traitez. En effet, la protection des données personnelles implique de mettre en place des « *mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque*[16].»

- L'utilisation des cartes CPS ?

La CPS doit rester **strictement personnelle**. En aucun cas, vous ne pouvez communiquer vos codes secrets à votre personnel.

Le personnel placé sous votre autorité doit également disposer d'une carte d'accès ou d'un mot de passe personnel conforme aux recommandations de la CNIL[17] (12 caractères comportant des chiffres, des lettres majuscules et minuscules, des caractères spéciaux), renouvelé régulièrement.

- Dois-je réaliser une analyse d'impact ?

L'analyse d'impact relative à la protection des données (AIPD) doit être réalisée pour les traitements de données personnelles susceptibles d'engendrer un risque élevé pour les droits et libertés des personnes concernées.

Ce n'est pas le cas de votre traitement.

La CNIL a sur ce point expressément visé dans la liste des traitements pour lesquels il n'est pas nécessaire de réaliser une analyse d'impact, les « *Traitements, mis en œuvre uniquement à des fins de ressources humaines et dans les conditions prévues par les textes applicables, pour la seule gestion du personnel des organismes qui emploient moins de 250 personnes, l'exception du recours au profilage*»[18].

[16] Article 24 du RGPD

[17] https://www.cnil.fr/fr/authentification-par-mot-de-passe-les-mesures-de-securite-elementaires

[18] https://www.cnil.fr/sites/default/files/atoms/files/liste-traitements-aipd-non-requise.pd

5) Comment informer votre personnel ?

- Modèle de note d'information à l'attention du personnel

Dans le cadre de la gestion de votre personnel, vous pouvez utiliser la mention d'information suivante et l'adapter à votre cas :

« Vos données personnelles font l'objet d'un traitement de données personnelles mis en œuvre par le cabinet [INDIQUER LE NOM DE VOTRE CABINET], en sa qualité de responsable de traitement, à des fins de gestion administrative du personnel et de la paie.

Elles sont destinées aux personnes habilitées chargées de la gestion du personnel, de la paie, des outils informatiques mis à votre disposition, et aux prestataires en charge de la paie, de la maintenance informatique agissant en qualité de sous-traitant. [CONSERVER UNIQUEMENT CE QUI EST APPLICABLE]

Elles sont également transmises aux organismes extérieurs autorisés (tels que les organismes de retraite, de prévoyance, ou autres assurances, diverses autorités réglementaires, etc.).

Dans ce contexte, vos données ne font l'objet d'aucun transfert en dehors de l'Union européenne.

Les données sont conservées pendant la durée nécessaire à leur traitement qui peut être, le cas échéant, fixée par les textes.

Conformément au Règlement européen général sur la protection des données du 27 avril 2016 et à la loi Informatique et Libertés modifiée, vous disposez d'un droit d'accès, de rectification, d'effacement de celles-ci ou une limitation du traitement aux données personnelles vous concernant en adressant un courrier électronique à l'adresse suivante : [adresse électronique] ou par courrier postal à : [adresse postale].

Vous disposez également, si vous l'estimez nécessaire, d'introduire une réclamation auprès de la Commission nationale Informatique et Libertés (CNIL). »

Cette information doit être donnée au moment de l'embauche du salarié et pour les salariés qui sont déjà en poste, il convient de leur adresser également cette note, soit en AR ou remise en mains propres contre signature pour avoir une trace de la transmission. Il y a également la possibilité d'insérer une clause dans son contrat (par avenant lorsqu'il s'agit d'un ancien salarié).

En pratique, cette mention d'information peut être transmise par mail afin de conserver la trace de cette communication.

- Comment réagir face à une demande d'exercice de droits d'un salarié ?

Chaque demande d'exercice d'un des droits précités doit être examinée dans les meilleurs délais, soit **dans un délai d'un mois à compter de la réception de la demande.**

Ce délai **peut être prolongé de deux mois**, au regard de la complexité et du nombre de demandes. Si tel est le cas, vous devez informer la personne concernée de cette prolongation et des motifs du report dans un délai d'un mois à compter de la réception de la demande.

6) Modèle prérempli de fiche de registre des traitements concernant vos collaborateurs

FICHE DE REGISTRE DE LA GESTION ADMINISTRATIVE DU PERSONNEL

Date de création de la fiche	
Date de dernière mise à jour de la fiche	
Nom du logiciel ou de l'application *(si pertinent)*	**Logiciel [Nom de votre application]**

Objectifs poursuivis

[Conserver uniquement les fonctionnalités mises en place.]

La gestion administrative des personnels :

- *gestion du dossier professionnel des employés ;*
- *gestion des annuaires internes et des organigrammes.*

La mise à disposition des personnels d'outils informatiques :

- *suivi et maintenance du parc informatique ;*
- *gestion des annuaires informatiques permettant de définir les autorisations d'accès aux applications et aux réseaux ;*
- *mise en œuvre de dispositifs destinés à assurer la sécurité et le bon fonctionnement des applications informatiques et des réseaux, à l'exclusion de tout traitement permettant le contrôle individuel de l'activité des employés ;*
- *gestion de la messagerie électronique professionnelle, à l'exclusion de tout traitement permettant le contrôle individuel de l'activité des employés.*

L'organisation du travail :

- *gestion des agendas professionnels ;*
- *gestion des tâches des personnels, à l'exclusion de tout traitement permettant un contrôle individuel de leur productivité.*

La formation des personnels :

- *suivi des demandes de formation et des périodes de formation effectuées ;*
- *organisation des sessions de formation ;*
- *évaluation des connaissances et des formations.*

La gestion de la paie

Catégories de personnes concernées

[Listez les différentes catégories de personnes concernées dont vous collectez ou utilisez les données.]

- salariés

Catégories de données collectées

[Cochez et listez les différentes données traitées.]

☒ État-civil, identité, données d'identification, images *(ex. nom, prénom, adresse, photographie, date et lieu de naissance, etc.)*

Précisez :

.....

☐ Vie personnelle *(ex. habitudes de vie, situation familiale, etc.)*

☒ Vie professionnelle *(ex. CV, situation professionnelle, scolarité, formation, distinctions, diplômes, etc.)*
Précisez :

.....

☒ Informations d'ordre économique et financier *(ex. revenus, situation financière, données bancaires, etc.)*
Précisez :

.....

☒Données de connexion *(ex. adresses Ip, logs, identifiants des terminaux, identifiants de connexion, informations d'horodatage, etc.)*

☐ Données de localisation *(ex. déplacements, données GPS, GSM, ...)*

☐ Internet *(ex. cookies, traceurs, données de navigation, mesures d'audience, ...)*

☐ Autres catégories de données *(précisez)* :

Des données sensibles sont-elles traitées ?

[La collecte de certaines données, particulièrement sensibles, est strictement encadrée par le RGPD et requiert une vigilance particulière. Il s'agit des données révélant l'origine prétendument raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale des personnes, des données génétiques et biométriques, des données concernant la santé, la vie sexuelle ou l'orientation sexuelle des personnes, des données relatives aux condamnations pénales ou aux infractions, ainsi que du numéro d'identification national unique (NIR ou numéro de sécurité sociale).]

☒ Oui ☐Non

Si oui, lesquelles ? : numéro de sécurité sociale pour la gestion de la paie

Durées de conservation des catégories de données

Combien de temps conservez-vous ces informations ?

Pour les bulletins de paie (double papier ou sous forme électronique) :
5..... ☐Jours ☐Mois ☒Ans

Pour le registre unique du personnel :
5..... ☐Jours ☐Mois ☒Ans

Pour les documents concernant les contrats de travail, salaires, primes, indemnités, soldes de tout compte, régimes de retraite :
5..... ☐Jours ☐Mois ☒Ans

Pour les documents relatifs aux charges sociales et à la taxe sur les salaires :
3..... ☐Jours ☐Mois ☒Ans

Pour la comptabilisation des horaires des salariés, des heures d'astreinte et de leur compensation :
1..... ☐Jours ☐Mois ☒Ans

Pour la déclaration d'accident du travail auprès de la caisse primaire d'assurance maladie :
5..... ☐Jours ☐Mois ☒Ans

Pour les autres données collectées dans le cadre de ce traitement, la durée de conservation correspond à la période d'emploi de la personne concernée.

Catégories de destinataires des données

Destinataires internes

1. les personnes habilitées chargées de la gestion du personnel (à conserver si applicable)

Organismes externes

1. organismes sociaux
2. organismes fiscaux
3. [A compléter si pertinent]

Sous-traitants

1. comptable (à conserver si applicable)
2. éditeur de logiciel [Nom de votre application] s'il assure une prestation de maintenance informatique ou d'hébergement de données (à conserver si applicable)
3. [A compléter si pertinent]

Transferts des données hors UE

Des données personnelles sont-elles transmises hors de l'Union européenne ?

☐ Oui ☒ Non

Mesures de sécurité

[Décrivez les mesures de sécurité cochées ci-dessous]

Le niveau de sécurité doit être adapté aux risques soulevés par le traitement. Les exemples suivants constituent des garanties de base à prévoir et peuvent devoir être complétés.

☒ Contrôle d'accès des utilisateurs

Décrivez les mesures : identifiant et mot de passe pour accéder à l'application utilisée dans le cadre de la gestion administrative des collaborateurs.

.....

☒ Mesures de traçabilité

Précisez la nature des traces *(exemple : journalisation des accès des utilisateurs),* les données enregistrées *(exemple : identifiant, date et heure de connexion, etc.)* et leur durée de conservation :

.....

☒ Mesures de protection des logiciels (antivirus, mises à jour et correctifs de sécurité, tests, etc.)

Décrivez les mesures : antivirus et mise à jour de l'application utilisée.

.....

☒ Sauvegarde des données

Décrivez les modalités :

.....

☐ Chiffrement des données

Décrivez les mesures (e*xemple : site accessible en https, utilisation de TLS, etc.)* :

.....

☒ Contrôle des sous-traitants (si applicable)

Décrivez les modalités : vérification des engagements pris par le(s) sous-traitant(s) au regard de l'article 28 du RGPD.

.....

☐ Autres mesures :

Information et respect des droits des personnes

Comment les personnes concernées sont informées du traitement ?

☒ Mention d'information

Précisez sur quel(s) support(s) : notice d'information communiquée lors de la signature du contrat avec la personne concernée

Comment sont traitées les demandes d'exercice des droits des personnes ?

Indiquez le délai du traitement de la demande : 1 mois

Indiquez la personne chargée de répondre aux demandes :

FICHE N°3 – Quelles sont vos obligations à l'égard de vos prestataires ?

Check-list des bonnes pratiques à respecter

- ⇨ Identifier la liste de vos prestataires qui sont amenés à traiter des données personnelles pour votre compte
- ⇨ Elaborer la fiche de registre relative à la gestion des prestataires
- ⇨ S'assurer que vos prestataires agissant en tant que sous-traitants présentent les garanties suffisantes en matière de sécurité et de confidentialité
- ⇨ Encadrer vos relations avec vos sous-traitants par la conclusion d'une clause de sous-traitance venant préciser les obligations de chacun en matière de protection des données personnelles

1) Qui sont vos sous-traitants ?

Dans le cadre de votre activité de pédicure-podologue, vous êtes amené à sous-traiter différentes prestations auprès de vos prestataires de services informatiques (hébergement, maintenance, infogérance), d'éditeurs de logiciels ou de comptables en charge de l'élaboration des bulletins de paie.

Toute personne qui traite des données personnelles au nom et pour le compte d'un autre organisme, dans le cadre d'un service ou d'une prestation est considérée comme un sous-traitant au sens de l'article 28 du RGPD.

Dans ce cas, vous devez encadrer vos relations par un contrat de sous-traitance.

2) Que doivent contenir les contrats avec vos sous-traitants ?

- Modèle de clause de sous-traitance pour les contrats à venir ou en cours

ANNEXE PROTECTION DES DONNEES PERSONNELLES

PREAMBULE

La présente annexe « Protection des Données personnelles » est partie intégrante au contrat de [objet des prestations à adapter : hébergement, maintenance informatique, infogérance, comptabilité, paie, etc.] (ci-après le « Contrat ») liant le CLIENT et le PRESTATAIRE.

Conformément au Contrat et dans le cadre de l'exécution de ses obligations, le PRESTATAIRE pourra être amené à traiter des Données Personnelles pour le compte du CLIENT. Le PRESTATAIRE agit en qualité de sous-traitant (ci-après le « Sous-traitant ») et le CLIENT agit en qualité de responsable du traitement (ci-après le « Responsable du traitement »).

En matière de protection des Données Personnelles, les Parties acceptent de se conformer aux dispositions de la présente Annexe.

Dans le cadre de la présente annexe, le Sous-traitant traite les données personnelles suivantes des [indiquer les catégories de personnes : patients, professionnels de santé, salariés, contacts, etc.] (ci-après les « **Personnes concernées** ») :

☐ Etat civil, données d'identification (par ex. nom prénom)

☐ Vie personnelle (situation familiale, habitude de vie…)

☐ Vie professionnelle (diplômes, spécialités, expérience, distinctions professionnelles…)

☐ Informations d'ordre économique et financier (coordonnées bancaires, moyens de paiement…)

☐ Données particulières (à détailler) :

☐ Autre, à préciser :

(ci-après les « **Données personnelles** »).

A LA SUITE DE QUOI, IL A ETE DECIDE CE QUI SUIT :

ARTICLE 1 : QUALIFICATION DES PARTIES

Chaque partie s'engage à garder strictement confidentielles et à ne pas divulguer à des tiers, par quelque moyen que ce soit, les informations qui lui seront transmises ou auxquelles elle aura accès à l'occasion de l'exécution du présent accord.

En particulier, les Parties s'engagent à collecter et traiter toute donnée personnelle en conformité avec la Réglementation applicable à la protection des données personnelles et en particulier le Règlement européen sur la protection des données du 27 avril 2016 (le « RGPD ») et la loi Informatique et Libertés modifiée (ci-après « la Réglementation applicable à la protection des données »).

ARTICLE 2 : OBLIGATIONS DU SOUS-TRAITANT

Le Sous-traitant s'engage à ne traiter les données que pour le compte du Responsable du traitement et sur ses seules instructions. Il informera le Responsable du traitement en cas d'instruction qui apparaîtrait contraire à la Réglementation applicable à la protection des données personnelles.

Le Sous-traitant prend toutes mesures techniques et organisationnelles appropriées afin de garantir la confidentialité des Données personnelles traitées et un niveau de sécurité conforme à la Réglementation applicable à la protection des Données personnelles. A ce titre, il s'engage à ce que les personnes autorisées à traiter les Données personnelles pour le compte du Responsable du traitement soient soumises à une obligation de confidentialité. En outre, le Sous-traitant s'engage à ne pas transférer les Données personnelles hors de l'Union européenne.

En cas de violation de Données personnelles au sens de la Réglementation applicable à la protection des données personnelles, le Sous-traitant s'engage à en informer le Responsable du traitement dans les meilleurs délais et au plus tard dans les 48 heures après en avoir eu connaissance.

Dans le cas où le Sous-traitant ferait appel à un sous-traitant ultérieur pour traiter les Données personnelles confiées par le Responsable du traitement, il s'engage à en l'informer et à ce que ce sous-traitant ultérieur soit soumis à des obligations au moins équivalentes à celles fixées par le présent Contrat et demeure pleinement responsable vis-à-vis du Responsable du traitement de l'exécution par ce sous-traitant ultérieur de ses obligations.

Le Sous-traitant met à la disposition du Responsable du traitement toute information nécessaire pour démontrer le respect des obligations décrites dans le présent Contrat et pour permettre la réalisation d'audits de conformité. Les Parties s'engagent à coopérer avec l'autorité de contrôle en matière de

protection des données personnelles en cas de demande d'information qui pourrait être adressée ou en cas de contrôle effectué.

Enfin, le Sous-traitant assistera le Responsable du traitement dans la mise en œuvre de l'exercice des droits des personnes concernées.

ARTICLE 3 : DUREE DE CONSERVATION ET RESTITUTION DES DONNEES

Le Sous-traitant s'engage à retourner au Responsable du traitement l'intégralité des Données personnelles des personnes concernées collectées pour le compte du Responsable du traitement et à supprimer définitivement toute copie restante de ces Données personnelles dans les quinze jours au terme du Contrat. Elle s'engage à communiquer, sur simple demande du Responsable du traitement, toute attestation de destruction de ces données.

ARTICLE 4 : RESPONSABILITE

Le Sous-traitant s'engage à indemniser le Responsable du traitement de tous dommages liés (i) à l'atteinte à la sécurité, l'intégrité ou à la confidentialité des Données personnelles résultant du manquement par Les Influenceurs de ses obligations au titre du présent contrat (ii) à toute violation de la Réglementation applicable à la protection des données personnelles et (iii) à tout préjudice d'image ou de réputation lié à un manquement du Sous-traitant à ses obligations au titre du présent Contrat.

ARTICLE 5 : LOI APPLICABLE

Le présent Contrat est soumis à la loi française.

Fait à

Le

En deux (2) exemplaires originaux. »

3) Quelles sont les obligations de vos sous-traitants ?

- Quel est son rôle en cas de violation des données ?

Le sous-traitant notifie au responsable de traitement toute violation de données à caractère personnel dans les meilleurs délais après en avoir pris connaissance[19]. Ce délai doit être compris entre 24h et 48h afin de permettre au responsable de traitement de notifier ladite violation à la CNIL dans le délai imparti, soit 72h après en avoir pris connaissance.

Cette notification est accompagnée de toute documentation utile afin de permettre au responsable de traitement, si nécessaire, de notifier cette violation à l'autorité de contrôle compétente.

- Quel est son rôle en cas d'analyse d'impact ?

Dans l'hypothèse où vous êtes tenu de réaliser une analyse d'impact (par exemple si vous mettez en œuvre un traitement de données sensibles à grande échelle) et que le traitement concerné fait appel à un sous-traitant, il doit vous aider, notamment en vous communiquant les informations nécessaires à la réalisation de l'analyse d'impact.

[19] Article 33.2 du RGPD

- Quel est son rôle en cas de demandes d'exercice de droit d'une personne ?

Dans la mesure du possible, le sous-traitant doit aider le responsable de traitement à s'acquitter de son obligation de donner suite aux demandes d'exercice des droits des personnes concernées[20], soit en leur répondant directement, soit en informant sans délai le responsable de traitement.

- Quel est son rôle en cas de contrôle de la CNIL ?

Le sous-traitant doit mettre à la disposition du responsable de traitement toutes les informations nécessaires pour démontrer le respect de ses obligations en cas de contrôle de la CNIL.

- Que se passe-t-il en cas de transfert des données hors Union Européenne ?

En cas de transferts de données en dehors de l'Union européenne, la Commission européenne a adopté des clauses contractuelles types permettant d'encadrer ces transferts.

Les clauses contractuelles encadrant les transferts de données personnelles d'un responsable de traitement à un sous-traitant établi dans les pays tiers à l'UE sont téléchargeables sur le site de la CNIL : https://www.cnil.fr/fr/les-clauses-contractuelles-types-de-la-commision-europeenne

- Que se passe-t-il à la fin du contrat ?

Au terme ou à la résiliation du contrat, vous pouvez demander à votre sous-traitant de supprimer les données personnelles et/ou de vous les restituer. En tout état de cause, le sous-traitant doit détruire les copies existantes, sauf si une obligation légale exige la conservation de celles-ci[21].

4) Modèle prérempli de fiche de registre concernant la gestion de vos prestataires

FICHE DE REGISTRE DE LA GESTION DES PRESTATAIRES

Date de création de la fiche	
Date de dernière mise à jour de la fiche	
Nom du logiciel ou de l'application *(si pertinent)*	**Logiciel [Nom de votre application]**

Objectifs poursuivis

[Conservez uniquement les fonctionnalités du traitement qui vous semblent pertinentes au regard de votre traitement]

Gestion des prestataires et des fournisseurs concernant les opérations administratives liées aux contrats, aux commandes, aux réceptions, aux factures, aux règlements, à la comptabilité pour ce qui a trait à la gestion des comptes prestataires.

Catégories de personnes concernées

[Listez les différents types de personnes dont vous collectez ou utilisez les données.]

- prestataires

[20] Article 28.2. e) RGPD
[21] Article 28.2. g) du RGPD

Catégories de données collectées

[Cochez et listez les différentes données traitées]

☒ État-civil, identité, données d'identification, images *(ex. nom, prénom, adresse, photographie, date et lieu de naissance, etc.)*

Nom ou raison sociale, prénoms, adresse (siège social, lieu de facturation), code d'identification comptable, téléphone, fax, adresse de courrier électronique, numéro SIREN.

☐ Vie personnelle *(ex. habitudes de vie, situation familiale, etc.)*

☒ Vie professionnelle *(ex. CV, situation professionnelle, scolarité, formation, distinctions, diplômes, etc.)*

Profession, catégorie économique, activité.

☒ Informations d'ordre économique et financier *(ex. revenus, situation financière, données bancaires, etc.)*

Eléments de la facturation et du règlement : les abonnements, article, produit, service faisant l'objet de l'abonnement, périodicité, montant, conditions :

- les commandes et les factures, articles, produits, services faisant l'objet de la commande et de la facture, quantité, prix, numéro, date et montant de la commande et de la facture, échéance de la facture, conditions de livraison ;
- paiement, conditions et modalités de règlement (moyen de paiement, références bancaires ou postales, remises, acomptes, ristournes), conditions de crédit, durée ;
- impayés, avoirs, reçus ;
- retenues ou oppositions.

☐ Données de connexion *(ex. adresses Ip, logs, identifiants des terminaux, identifiants de connexion, informations d'horodatage, etc.)*

☐ Données de localisation *(ex. déplacements, données GPS, GSM, ...)*

☐ Internet *(ex. cookies, traceurs, données de navigation, mesures d'audience, ...)*

☐ Autres catégories de données *(précisez)* :

Des données sensibles sont-elles traitées ?

La collecte de certaines données, particulièrement sensibles, est strictement encadrée par le RGPD et requiert une vigilance particulière. Il s'agit des données révélant l'origine prétendument raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale des personnes, des données génétiques et biométriques, des données concernant la santé, la vie sexuelle ou l'orientation sexuelle des personnes, des données relatives aux condamnations pénales ou aux infractions, ainsi que du numéro d'identification national unique (NIR ou numéro de sécurité sociale).

☐ Oui ☒ Non

Durées de conservation des catégories de données

Combien de temps conservez-vous ces informations ?

Pour les contrats conclus entre commerçants et entre commerçants et non-commerçants :

5..... ☐Jours ☐Mois ☒Ans

Pour la correspondance commerciale (bons de commandes, bons de livraison, etc.) :

10.....☐Jours ☐Mois ☒Ans

Pour les documents bancaires (relevés bancaires, talons de chèque, etc.) :

5..... ☐Jours ☐Mois ☒Ans

Pour les factures clients et/ou fournisseurs :

10.....☐Jours ☐Mois ☒Ans

Catégories de destinataires des données

Destinataires internes

1. les personnes habilitées

Organismes externes

1. les entreprises extérieures liées contractuellement pour l'exécution du contrat
2. les organismes publics, exclusivement pour répondre aux obligations légales
3. les auxiliaires de justice et les officiers ministériels dans le cadre de leur mission de recouvrement de créances
4. les organismes financiers teneurs des comptes mouvementés

Sous-traitants

1. comptable (à conserver si applicable)
2. éditeur de logiciel [Nom de votre application] s'il assure une prestation de maintenance informatique ou d'hébergement de données (à conserver si applicable)
3. [A compléter si pertinent]

Transferts des données hors UE

Des données personnelles sont-elles transmises hors de l'Union européenne ?

☐ Oui ☒ Non

Mesures de sécurité

Décrivez les mesures de sécurité cochées ci-dessous

Le niveau de sécurité doit être adapté aux risques soulevés par le traitement. Les exemples suivants constituent des garanties de base à prévoir et peuvent devoir être complétés.

☒ Contrôle d'accès des utilisateurs

Décrivez les mesures : identifiant et mot de passe pour accéder aux applications, y compris les applications bancaires pour effectuer les virements sur les comptes bancaires des prestataires.

.....

☒ Mesures de traçabilité

Précisez la nature des traces *(exemple : journalisation des accès des utilisateurs),* les données enregistrées *(exemple : identifiant, date et heure de connexion, etc.)* et leur durée de conservation :

.....

☒ Mesures de protection des logiciels (antivirus, mises à jour et correctifs de sécurité, tests, etc.)

Décrivez les mesures : antivirus et mise à jour de l'application ou des applications utilisées.

.....

☒ Sauvegarde des données

Décrivez les modalités :

.....

☐ Chiffrement des données

Décrivez les mesures (e*xemple : site accessible en https, utilisation de TLS, etc.)* :

.....

☒ Contrôle des sous-traitants (si applicable)

Décrivez les modalités : vérification des engagements pris par le(s) sous-traitant(s) conformément à l'article 28 du RGPD.

.....

☐ Autres mesures:

.....

Information et respect des droits des personnes

Comment les personnes concernées sont informées du traitement ? Cocher la ou les cases correspondantes :

☒ clause contractuelle

Comment sont traitées les demandes d'exercice des droits des personnes ?

Indiquez le délai du traitement de la demande : 1 mois

Indiquez la personne chargée de répondre aux demandes :

FICHE N°4 – Quelles sont vos obligations en cas d'installation d'un dispositif de vidéosurveillance ?

1) Dans quelles conditions pouvez-vous installer un dispositif de vidéosurveillance dans votre cabinet ?

Seul un intérêt légitime peut justifier l'installation de caméras dans votre cabinet. Par exemple, la nécessité d'assurer la sécurité des biens et des personnes au sein de votre cabinet et notamment, afin d'identifier les auteurs d'infractions (exemples : vols, dégradations, agressions).

Ce que vous pouvez faire	Ce que vous ne pouvez pas faire
• filmer les salariés qui manipulent de l'argent ou des biens de valeurs. • filmer les lieux de stocks, les réserves, les cuisines dédiées au personnel	• placer vos salariés sous une surveillance constante et permanente • filmer les zones de repos des salariés, les toilettes

Seules les personnes habilitées, dans le cadre de leurs fonctions, sont autorisées à visionner les images enregistrées par les dispositifs de vidéosurveillance. Sur ce point, vous devez sensibiliser les personnes qui accèdent aux images enregistrées aux règles de mises en œuvre d'un système de vidéosurveillance.

2) Quelles sont les formalités à accomplir préalablement à la mise en place d'un dispositif de vidéosurveillance ?

En fonction des lieux qui sont filmés, les formalités peuvent varier.

- Dispositif filmant un lieu ouvert ou non au public

Que les lieux filmés soient ouverts ou non au public, vous êtes tenu d'élaborer une fiche de registre relative à la vidéosurveillance dans la mesure où il s'agit d'un traitement de données personnelles. Sur ce point, une fiche de registre pré-remplie vous est proposée à la fin de cette fiche pratique.

- Pour les lieux non ouverts au public

Aucune formalité auprès de la CNIL n'est nécessaire à accomplir si les caméras que vous avez installées filment des locaux du cabinet qui ne sont pas ouverts au public, comme les lieux de stocks, les réserves, les cuisines dédiées au personnel.

Pour plus d'informations, vous pouvez consulter la fiche de la CNIL « La vidéosurveillance – vidéoprotection au travail ».

- Pour les lieux ouverts au public

Lorsque les caméras filment un lieu ouvert au public, comme les espaces d'entrées et de sorties, le dispositif mis en place doit être autorisé par le préfet du département.

Le formulaire de déclaration est accessible sur le site du ministère de l'Intérieur, vous pouvez y accéder ici : https://www.formulaires.service-public.fr/gf/cerfa_13806.do

Vous pouvez également procéder à une déclaration en ligne ici :
https://www.televideoprotection.interieur.gouv.fr/gup/PhpVideo/TeleDeclaration/cnxAccueil.php

3) Comment informer les personnes filmées ?

- Modèle de note d'information à l'attention des personnes filmées

La CNIL recommande deux niveaux d'informations.

✓ Niveau 1 de l'information : panneau d'information affiché dans les locaux du cabinet

« Etablissement placé sous vidéosurveillance par [Nom de votre cabinet] pour la sécurité des personnes et des biens.

Les images sont conservées pendant un mois et peuvent être visionnées, en cas d'incident, par le personnel habilité de [Nom de votre cabinet] et par les forces de l'ordre.

Conformément à la réglementation applicable à la protection des données, vous pouvez exercer votre droit d'accès aux images qui vous concernent ou demander toute information sur ce dispositif en écrivant à [*adresse email*] ou à l'adresse postale suivante : [*adresse postale du cabinet*].

Pour plus d'informations, nous vous invitons à consulter notre note d'information disponible à l'entrée du cabinet.

✓ Niveau 2 de l'information : dans la note d'information destinée à vos patients et à votre personnel

Le [Nom de votre cabinet] situé à [Adresse du cabinet] a placé ses locaux sous vidéosurveillance afin d'assurer la sécurité des personnes et de ses biens. En tant que responsable du traitement, le [Nom de votre cabinet] collecte des images des salariés et des patients. Le traitement de la vidéosurveillance est fondé sur l'intérêt légitime à des fins de sécurité, notamment pour lutter contre les vols et les agressions.

Les images enregistrées dans ce dispositif ne sont pas utilisées à des fins de surveillance du personnel, ni de contrôle des horaires.

Les images peuvent être visionnées, ***en cas d'incident****, par le personnel habilité de le [Nom de votre cabinet] et par les forces de l'ordre, ainsi que le personnel de la société en charge de la maintenance du matériel agissant en qualité de sous-traitant [CONSERVER SI APPLICABLE].*

Les images sont conservées pendant un mois à compter de leur enregistrement.

En cas d'incident lié à la sécurité des personnes et des biens, les images de vidéosurveillance peuvent néanmoins être extraites du dispositif. Elles sont alors conservées sur un autre support le temps du règlement des procédures liées à cet incident et accessibles aux seules personnes habilitées dans ce cadre.

Vous pouvez accéder aux données vous concernant où demander leur effacement. Vous disposez également d'un droit d'opposition et d'un droit à la limitation du traitement de vos données.

Pour exercer ces droits ou pour toute question sur le traitement de vos données, vous pouvez nous contacter par voie électronique [adresse e-mail] et par courrier postal [adresse postale de votre cabinet].

Vous disposez également, si vous l'estimez nécessaire, d'introduire une réclamation auprès de la Commission nationale Informatique et Libertés (CNIL).

Vous pouvez informer les personnes par la mise en place d'un panneau affiché en permanence, de façon visible dans les lieux filmés. Une icône peut être prévue afin de donner, de façon visible et intelligible, un aperçu significatif du traitement envisagé[22].

Pour plus d'informations, vous pouvez consulter la fiche de la CNIL « Exemple d'information pour un dispositif de vidéosurveillance sur les lieux de travail ».

4) Modèle prérempli de fiche de registre concernant votre dispositif de vidéosurveillance

FICHE DE REGISTRE DE LA GESTION DE LA VIDEOSURVEILLANCE

Date de création de la fiche	
Date de dernière mise à jour de la fiche	
Nom du logiciel ou de l'application *(si pertinent)*	**[Nom du dispositif utilisé]**

Objectifs poursuivis

[Décrivez clairement l'objet du traitement de données personnelles et ses fonctionnalités.]

Mise en place du dispositif de vidéosurveillance à des fins de sécurité, notamment pour lutter contre les vols et les agressions.

Catégories de personnes concernées

[Listez les différents types de personnes dont vous collectez ou utilisez les données.]

[22] https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_201903_videosurveillance.pdf

- salariés
- patients

Catégories de données collectées

[Cochez et listez les différentes données traitées]

☒ État-civil, identité, données d'identification, images *(ex. nom, prénom, adresse, photographie, date et lieu de naissance, etc.)*

☐ Images

☐ Vie personnelle *(ex. habitudes de vie, situation familiale, etc.)*

☐ Vie professionnelle *(ex. CV, situation professionnelle, scolarité, formation, distinctions, diplômes, etc.)*

☐ Informations d'ordre économique et financier *(ex. revenus, situation financière, données bancaires, etc.)*

☐ Données de connexion *(ex. adresses Ip, logs, identifiants des terminaux, identifiants de connexion, informations d'horodatage, etc.)*

☐ Données de localisation *(ex. déplacements, données GPS, GSM, ...)*

☐ Internet *(ex. cookies, traceurs, données de navigation, mesures d'audience, ...)*

☐Autres catégories de données *(précisez)* :

Des données sensibles sont-elles traitées ?

La collecte de certaines données, particulièrement sensibles, est strictement encadrée par le RGPD et requiert une vigilance particulière. Il s'agit des données révélant l'origine prétendument raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale des personnes, des données génétiques et biométriques, des données concernant la santé, la vie sexuelle ou l'orientation sexuelle des personnes, des données relatives aux condamnations pénales ou aux infractions, ainsi que du numéro d'identification national unique (NIR ou numéro de sécurité sociale).

☐ Oui ☒ Non

Durées de conservation des catégories de données

Combien de temps conservez-vous ces informations ?

Les données sont conservées pendant un mois à compter de leur enregistrement.

Catégories de destinataires des données

Destinataires internes

- personnes habilitées
- [A compléter si pertinent]

Organismes externes

- les personnes dépositaires de l'autorité publique
- [A compléter si pertinent]

Sous-traitants

- le prestataire qui a installé le dispositif de vidéosurveillance (s'il accède aux images)
- [A compléter si pertinent]

Transferts des données hors UE

Des données personnelles sont-elles transmises hors de l'Union européenne ?

☐ Oui ☒Non

Mesures de sécurité

[Cochez et décrivez les mesures de sécurité organisationnelles et techniques prévues pour préserver la confidentialité des données.]

Le niveau de sécurité doit être adapté aux risques soulevés par le traitement. Les exemples suivants constituent des garanties de base à prévoir et peuvent devoir être complétés.

☒ Contrôle d'accès des utilisateurs

Décrivez les mesures : identifiant et mot de passe pour accéder à l'application.

☒ Mesures de traçabilité

Précisez la nature des traces *(exemple : journalisation des accès des utilisateurs),* les données enregistrées *(exemple : identifiant, date et heure de connexion, etc.)* et leur durée de conservation :

.....

☒ Mesures de protection des logiciels (antivirus, mises à jour et correctifs de sécurité, tests, etc.)

Décrivez les mesures : antivirus et mise à jour de l'application utilisée.

.....

☒ Sauvegarde des données

Décrivez les modalités :

.....

☐ Chiffrement des données

Décrivez les mesures (e*xemple : site accessible en https, utilisation de TLS, etc.)* :

.....

.....

☒ Contrôle des sous-traitants (si applicable)

Décrivez les modalités : vérification des engagements pris par le sous-traitant au regard de l'article 28 du RGPD (dans l'hypothèse où le sous-traitant accède aux images).

.....

☐ Autres mesures :

Information et respect des droits des personnes

Comment les personnes concernées sont informées du traitement ?

☒ Panneau d'information et notice d'information

Comment sont traitées les demandes d'exercice des droits des personnes ?

Indiquez le délai du traitement de la demande : 1 mois

Indiquez la personne chargée de répondre aux demandes :

IV. GLOSSAIRE (par ordre alphabétique)

Destinataire : la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui reçoit communication de données à caractère personnel, qu'il s'agisse ou non d'un tiers. Toutefois, les autorités publiques qui sont susceptibles de recevoir communication de données à caractère personnel dans le cadre d'une mission d'enquête particulière conformément au droit de l'Union ou au droit d'un État membre ne sont pas considérées comme des destinataires ; le traitement de ces données par les autorités publiques en question est conforme aux règles applicables en matière de protection des données en fonction des finalités du traitement.

Donnée personnelle : toute information se rapportant à une personne physique identifiée ou identifiable (ci-après dénommée «personne concernée») ; est réputée être une «personne physique identifiable» une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale.

Fichier : tout ensemble structuré de données à caractère personnel accessibles selon des critères déterminés, que cet ensemble soit centralisé, décentralisé ou réparti de manière fonctionnelle ou géographique.

Responsable du traitement : la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement ; lorsque les finalités et les moyens de ce traitement sont déterminés par le droit de l'Union ou le droit d'un État membre, le responsable du traitement peut être désigné ou les critères spécifiques applicables à sa désignation peuvent être prévus par le droit de l'Union ou par le droit d'un État membre.

Sous-traitant : la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement.

Traitement : toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction.

Violation de données à caractère personnel : une violation de la sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou l'accès non autorisé à de telles données.

116 rue de la Convention
75015 PARIS
Tél. +33 1 45 54 53 23
Fax +33 1 45 54 53 68

www.onpp.fr

ORDRE NATIONAL
DES PÉDICURES-PODOLOGUES