CHIRURGIENS-DENTISTES, PRÉPAREZ-VOUS AU RGPD

Depuis le 25 mai dernier, le règlement général sur la protection des données (RGPD) est en vigueur. Ce texte vise à améliorer la gestion des données personnelles par les entreprises privées et publiques dans l'Union. Le chirurgien-dentiste est directement impacté. Mode d'emploi.

Un nouveau règlement européen instaure, depuis le 25 mai dernier, des obligations et des droits sur la manière dont les données personnelles sont collectées et traitées. Ainsi, le règlement général sur la protection des données personnelles (RGPD) s'applique à tous les organismes, tant privés que publics, et à tous les champs d'activité, y compris le domaine dentaire [1]. *« Le secteur de la santé est d'autant plus impacté par ce texte que les données de santé bénéficient d'un régime de protection renforcée car elles sont considérées comme des données sensibles »*, rappelle la Commission nationale de l'informatique et des libertés (Cnil) qui précise : *« À cela s'ajoutent les obligations additionnelles prévues par le Code de la santé publique (CSP), relatives aux données couvertes par le secret médical (règles relatives à l'hébergement externalisé des données de santé, à la télémédecine, à l'identifiant national de santé, etc.). »* Pour permettre aux chirurgiens-dentistes de se conformer au RGPD, nous proposons dans les pages suivantes un dossier pratique en 22 questions-réponses. >>>

L'ORDRE SE CONFORME AU RGPD

Pour respecter les obligations inscrites au RGPD, le Conseil national a désigné un délégué à la protection des données *(DPO)*. Celui-ci devra s'assurer de la mise en conformité avec le RGPD de l'instance ordinale, garantir une protection optimale des données et être en mesure de la démontrer. Le *DPO* exercera une mission d'information, de conseil et de contrôle en interne.

Qu'est-ce que le RGPD ?

Le sigle RGPD signifie *« règlement général sur la protection des données »*. Entré en vigueur le 25 mai dernier, le RGPD encadre le traitement des données personnelles au sein de l'Union. Ce règlement harmonise les règles en Europe en offrant un cadre juridique commun aux professionnels. De plus, pour mettre fin à une distorsion de concurrence entre des pays membres de l'UE et des pays tiers, les mêmes obligations sont imposées aux entreprises établies hors UE dès lors qu'elles proposent des produits ou des services aux Européens.

Quel est le champ d'application du RGPD ?

Le RGPD s'applique aux traitements, automatisés ou non, de données à caractère personnel, réalisés sur support informatique (logiciels, applications, bases de données, sites Web, etc.), mais également sur support papier.

Le RGPD concerne-t-il les chirurgiens-dentistes ?

Oui. Les praticiens sont directement concernés par le RGPD puisqu'ils sont amenés à traiter des données personnelles « sensibles », c'est-à-dire les données de santé. Pour cette catégorie de données, les chirurgiens-dentistes doivent tenir compte à la fois des dispositions du RGPD et de celles qui sont spécifiques au droit de la santé français. Enfin, cette nouvelle législation européenne impose aux praticiens d'assurer une protection optimale des données à chaque instant et d'être en mesure de la démontrer en documentant leur conformité au RGPD.

Comment se mettre en conformité avec le RGPD ?

Les chirurgiens-dentistes doivent tenir une documentation sur le traitement qu'ils réservent aux données personnelles et s'assurer que ce dernier respecte bien les nouvelles obligations légales du RGPD. Désormais, la mise en conformité d'un traitement de données personnelles passe principalement par la tenue d'un registre [2]. Le praticien est le *« responsable du traitement »*, dont il détermine les finalités et les moyens. Autrement dit, le praticien doit être en mesure de démontrer qu'il respecte le RGPD *via* ce registre des activités de traitement *(lire l'encadré « Registre, ce que dit le règlement », p. 26)*.

Quelle forme doit prendre le registre ?

Le registre doit se présenter sous une forme écrite qui autorise le format électronique. Il doit être mis à la disposition de la Cnil sur demande. La Cnil propose en téléchargement un modèle de registre des activités de traitement depuis l'adresse *https://www.cnil.fr/fr/rgpd-et-tpepme-un-nouveau-modele-de-registre-plus-simple-et-plus-didactique*. L'Ordre travaille sur l'adaptation spécifique de ce modèle à notre profession afin de faciliter sa prise en main et sa tenue. *La Lettre* y reviendra dans un prochain numéro.

Quelles informations doit contenir le registre ?

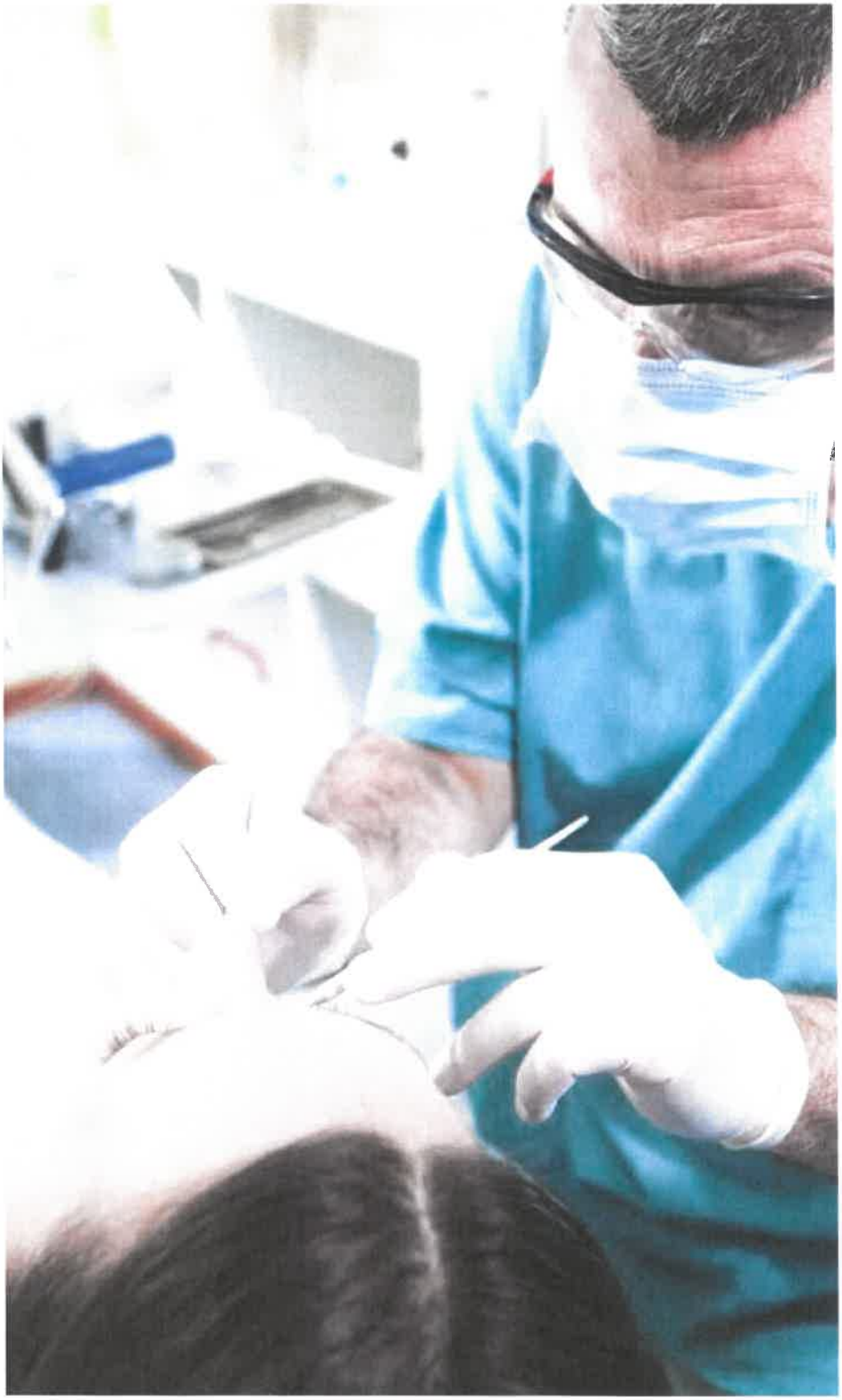
Le registre doit comporter les informations suivantes :

- Le nom et les coordonnées du praticien ;
- Les finalités du traitement (par exemple la télétransmission) ;
- Une description des catégories de personnes concernées (par exemple les patients, les employés) ;
- Une description des catégories de données personnelles (par exemple les données de santé, l'identité, la situation familiale) ;
- Les catégories de destinataires auxquels les données sont communiquées (par exemple la sécurité sociale, le patient) ;

• La durée de conservation des données (par exemple 20 ans pour les données de santé) ;
• Une description des mesures de sécurité mises en place par le praticien.
À noter que pour chaque activité impliquant le traitement de données personnelles, le praticien doit créer et tenir à jour une fiche de registre (par exemple la gestion de la paie, la gestion des fournisseurs, la gestion des patients, etc.).

La tenue d'un registre suffit-elle ?

Non. Parallèlement, le praticien doit aussi vérifier si les traitements de données personnelles répondent aux conditions de sécurité posées par le RGPD. Par exemple, il doit observer scrupuleusement :
• Le principe de minimisation des données (seules les données nécessaires au traitement sont collectées) ;
• Les modalités de collecte du consentement et de transparence (vérifier les mentions d'information et les clauses contractuelles relatives aux traitements de données personnelles mis en œuvre dans le cadre des relations avec les patients et les salariés) ;
• Les mentions obligatoires dans les contrats avec les sous-traitants ;
• Les mesures (organisationnelles, techniques) garantissant la sécurité des données afin d'éviter leur destruction, leur perte, leur altération ou leur divulgation non autorisée. Sur ce point, l'Ordre invite les praticiens à consulter le *Mémento de sécurité informa-* »»»



REGISTRE, CE QUE DIT LE RÈGLEMENT

La tenue du registre d'activité de traitement est obligatoire pour toutes les entreprises – dont les cabinets dentaires – qui traitent les données dites *« sensibles »* visées à l'article 9 du règlement, c'est-à-dire *« les données à caractère personnel qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale [...] »*. Le traitement de ces informations de même que celui *« des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique sont interdits »*.

>>> *tique pour les professionnels de santé en exercice libéral*, qui répond à la politique générale de sécurité des systèmes d'information de santé (PGSSI-S) [3] définie par l'Agence des systèmes d'information partagés de santé (Asip Santé). Le mémento aide le praticien à respecter ses obligations légales. Il permet aussi d'éviter de nombreux écueils pouvant aller jusqu'à la perte des données de santé contenues dans les systèmes informatiques.

Quel accès le patient a-t-il à ses données personnelles ?

En application du RGPD, lorsque des données personnelles d'une personne sont collectées auprès d'elle, le praticien doit lui délivrer de façon concise, transparente, compréhensible et accessible les trois niveaux d'information suivants :

1. L'identité et les coordonnées du responsable du traitement ;
2. Les finalités du traitement ;
3. Les potentiels destinataires des données personnelles, ou l'intention du praticien d'effectuer un transfert des données vers un pays tiers ou une organisation internationale ;

Pour garantir un traitement équitable et transparent, le praticien doit également fournir au patient les informations suivantes : droit d'accès et de rectification, droit à l'oubli, droit à la portabilité des données, droit de réparation des dommages, matériels ou moraux, droit d'effacement, droit à la limitation du traitement, droit d'opposition, principe des actions collectives et conditions particulières du traitement des données pour les mineurs de moins de 16 ans.

Rappelons que ces informations doivent être fournies au patient en des termes clairs et simples, en particulier lorsqu'elles sont destinées à un enfant. Elles peuvent être délivrées aussi bien par écrit que par voie électronique.

Attention : toutes les dispositions du RGPD et du Code de la santé publique ne sont pas harmonisées. En effet, le CSP prévoit des règles spécifiques en matière de données de santé auxquels les praticiens doivent se conformer. »»»

SIX RÉFLEXES POUR PROTÉGER LES DONNÉES PERSONNELLES

Collecter et traiter des données personnelles implique d'informer les personnes sur la façon dont le chirurgien-dentiste les exploite et de respecter leurs droits.
En tant que responsable de leur traitement, le praticien doit prendre des mesures pour garantir que l'utilisation de ces données se fera dans le respect de la vie privée des personnes concernées.

1. NE COLLECTER QUE LES DONNÉES VRAIMENT NÉCESSAIRES

Se poser les bonnes questions : Quel est mon objectif ? Quelles données sont indispensables pour l'atteindre ? Ai-je le droit de les collecter ? Est-ce pertinent ? Les personnes concernées ont-elles donné leur accord ?

2. ÊTRE TRANSPARENT

Une information claire et complète constitue le socle du contrat de confiance qui lie le praticien à ses patients.

3. PENSER AUX DROITS DES PERSONNES

Le praticien doit répondre dans les meilleurs délais aux demandes de consultation, de rectification ou de suppression des données.

4. GARDER LA MAÎTRISE DES DONNÉES

Le partage et la circulation des données personnelles doivent être encadrés et contractualisés pour permettre leur protection à tout moment.

5. IDENTIFIER LES RISQUES

Le praticien traite des données sensibles : des mesures spécifiques s'appliquent.

6. SÉCURISER VOS DONNÉES

Les mesures de sécurité, informatique mais aussi physique, doivent être adaptées en fonction de la sensibilité des données et des risques qui pèsent sur les personnes en cas d'incident.

LE GLOSSAIRE DU RGPD

DONNÉES À CARACTÈRE PERSONNEL

La notion de *«données personnelles»* s'entend de façon très large. Une donnée personnelle correspond à *«toute information se rapportant à une personne physique identifiée ou identifiable»*. Une personne peut être identifiée :

- directement (par ses nom et prénom, par exemple) ;
- indirectement, notamment par un identifiant tel que le numéro client, un numéro de téléphone, une donnée biométrique, plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale, mais aussi par sa voix ou son image ;

L'identification d'une personne physique peut être réalisée :

- à partir d'une seule donnée (par exemple le numéro de sécurité sociale, l'ADN) ;
- à partir du croisement d'un ensemble de données (par exemple une femme domiciliée à telle adresse, née tel jour, abonnée à tel magazine et militant dans telle association).

DONNÉES CONCERNANT LA SANTÉ

Le RGPD stipule que les données de santé sont des *«données à caractère personnel relatives à la santé physique ou mentale d'une personne physique, y compris la prestation de services de soins de santé, qui révèlent des informations sur l'état de santé de cette personne»*. Le texte précise que les données de santé peuvent se rapporter à l'état de santé (passé, présent ou futur) d'une personne, par exemple les données collectées dans un contexte médical (prestation de soins de santé, résultats de tests, etc.) ainsi que les données permettant d'identifier une maladie ou un risque de maladie, un handicap, des antécédents médicaux, un traitement clinique, un état psychologique ou biomédical. Les données génétiques et biométriques trouvent également une définition dans le texte européen.

TRAITEMENT DE DONNÉES PERSONNELLES

Un traitement de données personnelles est une opération, ou un ensemble d'opérations, portant sur des données personnelles, quel que soit le procédé utilisé (collecte, enregistrement, organisation, conservation, adaptation, modification, extraction, consultation, utilisation, destruction, communication par transmission, diffusion ou toute autre forme de mise à disposition...). Un traitement de données personnelles n'est pas nécessairement informatisé : les fichiers papier sont également concernés et doivent être protégés dans les mêmes conditions. Un traitement de données doit avoir un objectif, une finalité : il est ainsi interdit de collecter ou de traiter des données personnelles dans la perspective de leur éventuelle utilité future. À chaque traitement de données doit être assigné un but, qui doit bien évidemment être légal et légitime au regard de notre activité professionnelle.

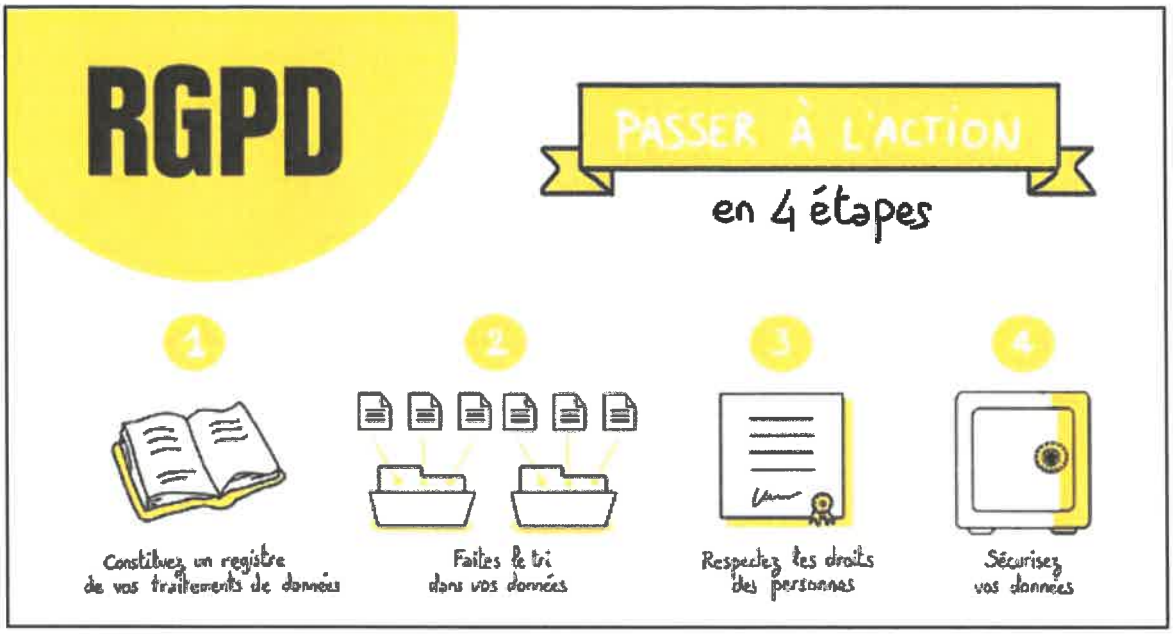
RESPONSABLE DU TRAITEMENT

Il s'agit, sauf désignation expresse par des dispositions législatives ou réglementaires, de la personne de l'autorité publique, du service ou de l'organisme qui détermine les finalités (ce à quoi sert le traitement) ou les moyens (permettant de répondre à cet objectif) d'un traitement de données personnelles. Le responsable du traitement est tenu de respecter l'ensemble des obligations découlant de la loi Informatique et Libertés et du RGPD (notamment l'information et l'éventuel recueil du consentement de la personne concernée, la mise en place de mesures de sécurité adaptées et, le cas échéant, la réalisation des formalités préalables auprès de la Cnil).

SOUS-TRAITANT

Le sous-traitant est toute personne, organisme ou autorité à qui le responsable du traitement a confié la réalisation de tout ou partie du traitement. Il collecte et traite les données uniquement au nom et pour le compte du responsable du traitement et sur instruction de celui-ci.

Par exemple, lorsqu'un établissement d'hébergement ou de soins propose un dispositif permettant à ses résidents de générer une alerte en cas de chute et recourt à une société tierce pour les équiper, l'établissement est considéré comme responsable du traitement, et la société tierce comme sous-traitant.



Capture d'écran du site Internet de la Cnil qui détaille les quatre actions principales à mener pour entamer sa mise en conformité aux règles de protection des données du RGPD.

Un cabinet dentaire doit-il avoir un délégué à la protection des données (DPO) ?

Non. Pour les praticiens exerçant en individuel ou au sein de cabinets dentaires de groupe, il n'est pas obligatoire de désigner un DPO *(lire l'encadré « L'Ordre se conforme au RGPD », p. 24)*. Voici les cas où la désignation d'un DPO est obligatoire :

- Si la structure appartient au secteur public ;
- Si les activités principales de la structure amènent à réaliser un suivi régulier et systématique des personnes à grande échelle ;
- Si les activités principales de la structure l'amènent à traiter, toujours à grande échelle, des données « sensibles » ou des données relatives aux condamnations.

LES ARNAQUES AU RGPD SE MULTIPLIENT

La Cnil dénonce les agissements de sociétés promettant de manière peu scrupuleuse une mise en conformité *« clé en main »* avec le RGPD. Leur technique consiste à insister sur les sanctions financières encourues, à se présenter comme « labellisées », « certifiées » ou « recommandées » par la Cnil et à adresser aux praticiens une simple documentation. C'est pourquoi la Cnil et l'Ordre appellent une nouvelle fois à la vigilance et rappellent que de tels démarchages ne se font pas à l'initiative de la Cnil. Si un praticien met en doute la probité d'un démarchage, l'Ordre l'invite à prendre contact au plus tôt avec la Cnil au 01 53 73 22 22.

Qu'est-ce que le droit à la portabilité des données ?

Le RGPD prévoit que les patients ont le droit d'obtenir du praticien une copie de leurs données personnelles qui font ou ont fait l'objet d'un traitement. Le règlement exige que ces données soient remises *« dans un format structuré, couramment utilisé [et] lisible par machine »*.

En d'autres termes, ces données « portables » doivent pouvoir être extraites et/ou être réutilisées facilement par la personne concernée. Ce droit existe déjà au regard de l'article R. 1111-2 du Code de la santé publique qui organise l'accès au patient des éléments contenus dans son dossier médical. »»»

Quelle est la durée de conservation des données de santé ?

En l'absence de règles propres au dossier constitué par le chirurgien-dentiste pour le suivi de ses patients, il est d'usage d'adopter une durée de conservation de 20 ans à compter des derniers soins et jusqu'au 28e anniversaire pour un mineur. Cette durée est prévue à l'article R. 1112-7 du Code de la santé publique. Le *Mémento de sécurité informatique pour les professionnels de santé en exercice libéral* de l'Asip Santé [3] peut être consulté pour obtenir des informations complémentaires.

Comment garantir la sécurité et la confidentialité des données ?

Avant l'application du RGPD, le praticien devait déjà garantir l'intégrité de son patrimoine de données en minimisant les risques de perte de données ou de piratage. Pour rappel, les mesures à prendre dépendent de la sensibilité des données traitées et des risques qui pèsent sur les personnes en cas d'incident. Différentes actions doivent être mises en place, dont les mises à jour des antivirus et des logiciels, l'utilisation de mots de passe complexes et leur changement régulier. En cas de perte ou vol d'un outil informatique, il sera plus difficile pour un tiers d'y accéder. Les documents de la PGSSI-S sont des guides de référence et fournissent des recommandations importantes s'agissant de la sécurité des données [4]. L'Ordre invite vivement les chirurgiens-dentistes à les consulter.

Le consentement du patient est-il indispensable ?

Si la question n'est pas encore totalement tranchée par la Cnil d'un point de vue juridique, nous retiendrons cependant que le praticien peut collecter, utiliser et traiter des données personnelles lorsque le traitement est nécessaire à la sauvegarde des intérêts vitaux du patient (une urgence, par exemple), à l'exécution d'un contrat (auquel la personne est partie), au respect d'une obligation légale à laquelle le responsable est soumis, à l'exécution d'une mission d'intérêt public, etc.

Et pour le patient mineur ?

Les titulaires de l'autorité parentale sont informés des traitements de données de santé portant sur leur enfant mineur, lequel reçoit également une information spécifique et adaptée. Attention : dans certains cas de figure, des dispositions spécifiques auront vocation à s'appliquer.

La CCAM est-elle une donnée de santé ?

Oui, si l'information découlant de ce codage conduit à délivrer une information sur l'état de santé ou sur une prise en charge en lien avec une pathologie particulière.

Le numéro de sécurité sociale constitue-t-il une donnée personnelle ?

Oui. Le numéro de sécurité sociale est unique et permet d'identifier un individu de manière certaine. Il s'agit donc d'une donnée personnelle sensible nécessitant des garanties supplémentaires et qui ne peut être traitée ou collectée arbitrairement.

Qu'en est-il de la gestion de la paie de ses salariés à un tiers ?

Elle est impactée par le RGPD. Lorsque la gestion de la paie ou le stockage du bulletin de paie (notamment par l'utilisation de coffres-forts numériques) sont confiés à un tiers, le praticien demeure responsable du traitement, mais le prestataire est également soumis au RGPD en tant que sous-traitant.

Le praticien doit-il obtenir le consentement de ses salariés ?

Non. Le traitement des données personnelles d'un salarié est nécessaire à l'exécution du contrat de travail. Son consentement n'est donc pas nécessaire.

Le praticien est-il responsable des données confiées à ses sous-traitants ?

Oui. Le praticien est responsable du traitement des données personnelles qu'il collecte ou qu'il utilise. En revanche, dans le cas où il confie la gestion ou le traitement de ces données à des tiers (partenaires, prestataires ou sous-traitants), ces derniers peuvent être considérés comme des sous-traitants au sens du RGPD (avec des obligations). Ainsi, dès que le praticien a recours à un prestataire de services dont la prestation implique le traitement de données de santé, il doit si- »»»

gner avec lui un contrat décrivant précisément le contenu de la prestation (obligation de sécurité et respect des clauses prévues par l'article 28 du RGPD).

Le RGPD s'applique-t-il aux données anonymisées ?

Non. Il s'applique aux données «pseudonymisées» qui, par un ensemble de recoupements, peuvent permettre d'identifier une personne. L'anonymisation suppose que l'identification de la personne est rendue impossible ou difficile compte tenu des coûts, du temps nécessaire ou des technologies disponibles.

En cas d'incident de sécurité, le praticien doit-il alerter la Cnil ?

Oui. En cas d'incident de sécurité (accès non autorisé, fuite ou perte de données, par exemple) susceptible d'engendrer un risque pour les droits des personnes concernées, le praticien doit le notifier à la Cnil. Cette notification doit intervenir dans un délai de 72 heures à compter de la découverte de l'incident, c'est-à-dire à partir du moment où le praticien est certain qu'une faille de sécurité sur ses systèmes informatiques s'est produite et que des données personnelles ont été impactées. La notification peut être dédoublée : le responsable informe la Cnil dans un premier temps avant de fournir des informations plus complètes et détaillées de l'incident dans un second temps.

Des sanctions sont-elles prévues en cas de non-conformité ?

Oui, mais on peut raisonnablement estimer que les premiers organismes à être contrôlés seront les géants du Web, friands de données personnelles. Cependant, la Cnil indique sur son site Internet que les responsables de traitement et les sous-traitants peuvent faire l'objet de lourdes sanctions administratives en cas de méconnaissance des dispositions du règlement. ■

(1) Le texte du RGPD est consultable à partir du lien *http://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:32016Rw0679&from=FR*

(2) Les formalités déclaratives auprès de la Cnil sont supprimées. Il n'est ainsi plus nécessaire de procéder à une déclaration du traitement auprès de cet organisme.

(3) Le mémento peut être téléchargé à partir de l'adresse *http://esante.gouv.fr/sites/default/files/Memento_Securite.pdf*

(4) Les documents sont consultables à partir de l'adresse *http://esante.gouv.fr/pgssi-s/espace-publication*