Association Française des Vétérinaires pour Animaux de Compagnie

Le Règlement général de protection des données (RGPD) : application à la clinique vétérinaire

Christophe Lebis

Partenaires privilégiés du Groupe d'étude et de recherche en management

Le Règlement général de protection des données (RGPD) : application à la clinique vétérinaire

Groupe d'Etude et de Recherche en Management – AFVAC

Avril 2019

Auteur :

Christophe Lebis

DV, CES Dermatologie, DEUST médias interactifs et communicants.

Remerciements à Jacques Foucault, Consultant formateur RGPD, pour l'autorisation de partage des modèles de documents (fiche de traitement, politique de sécurité, politique de protection et contrat de sous-traitance).

Remerciements également aux partenaires privilégiés du GERM pour leur soutien à leur action :

DIGIVET innove au service de votre passion et de votre performance ! Grâce à un ensemble de solutions simples et interconnectées pour améliorer la performance de la clinique, les vétérinaires et ASV peuvent consacrer plus de temps au soin de l'animal et optimiser la relation au propriétaire.

Depuis la création du GERM, Hill's est engagé auprès du groupe pour promouvoir auprès des vétérinaires la connaissance des différentes disciplines du management. Nous sommes convaincus, qu'au-delà de la nutrition, une solide expertise en gestion participe au développement de l'activité des cliniques.

Sommaire

Le Règlement général de protection des données (RGPD) est un règlement adopté par le parlement européen en avril 2016 et applicable dans l'ensemble de l'Union européenne depuis le 25 mai 2018. Il ne s'agit donc pas d'une décision récente, mais beaucoup d'entreprises ont pris du retard dans son application.

Bases et principes

L'objectif du RGPD est de protéger les personnes physiques à l'égard du traitement de leurs données à caractère personnel (DCP), et de faire respecter leur liberté et leurs droits. Il ne s'agit pas de notions nouvelles. En France, la loi Informatique et Liberté de 1978 avait déjà cette finalité. Finalement, on peut dire que le RGPD n'est qu'une extension de cette loi à l'ensemble de l'Union européenne, avec des modalités d'application différentes. A noter que ce règlement laisse la possibilité aux états membres d'apporter des précisions ou des limitations.

Qui est concerné ?

Toutes les personnes morales ou physiques détentrices de données à caractère personnel. La naissance de ce règlement est issu d'un désir de limitation de l'emprise de certaines grandes sociétés internationales (les fameuses GAFAM – Google, Amazon, Facebook, Apple, Microsoft) sur les DCP de centaines de millions de personnes et de leur exploitation sans scrupules. Mais ce règlement s'applique bien à tous, et même si les vétérinaires ne seront sans doute pas parmi les premiers contrôlés, il est nécessaire d'en avoir conscience, d'autant que les sanctions en cas de non-respect sont sévères (jusqu'à 4 % du chiffre d'affaires ou 20 millions d'euros).

Pas de panique cependant. La CNIL, chargée du contrôle de l'application du RGPD en France, a précisé qu'elle aurait, particulièrement dans les premiers temps, essentiellement un rôle d'accompagnement pour les TPE et PME, surtout si celles-ci avaient fait l'effort d'initier la constitution de leur dossier RGPD. Les sanctions n'arriveront que dans un seconde temps.

Définitions

Données à caractère personnel (DCP) : toute information relative à une personne physique identifiée ou qui peut être identifiée directement ou indirectement. On distingue trois types de DCP : les DCP classiques, les DCP à risque et les DCP sensibles. Ces dernières regroupent des informations très personnelles : santé, orientation sexuelle, politique, religieuse… données qu'une structure vétérinaire ne doit pas posséder. Les éléments constitutifs de la personnalité (nom, prénom), les adresses et numéros, les données sociologiques, les données des animaux possédés et leur suivi sont des données personnelles, à partir du moment où elles

peuvent être rattachées à une personne. A contrario, le traitement de données sociologiques ou épidémiologiques anonymisées n'entre pas dans le cadre du RGPD.

Traitement de données : toute action de manipulation de données : établissement de factures, envoi de mails… La collecte des données et leur hébergement sont des traitements. La loi concerne aussi bien les données stockées numériquement que sur papier.

Responsable de traitement : la personne physique ou morale qui détermine la finalité du traitement. Les associés d'une clinique qui constitue un fichier client dans le but par exemple d'éditer des factures sont les responsables de traitement.

Délégué à la protection des données (Data Protection Officer - DPO) : personne responsable de la protection des données au sein de la société. La nomination et la déclaration d'un DPO auprès de la CNIL est obligatoire dans un certain nombre de cas : possession de données sensibles, traitement à grande échelle, surveillance des personnes... Ceci ne concerne (normalement !) pas les structures vétérinaires, qui peuvent se contenter de nommer un membre de l'équipe "référent DPO". A défaut, le référent DPO sera le chef d'entreprise. Son rôle sera de piloter la mise en conformité de la structure vis-à-vis du RGPD, de sensibiliser le personnel à la confidentialité des données et à leur sécurité, de prioriser les urgences, de suivre l'évolution des politiques et des outils dans le temps. Cependant, cette personne n'est pas responsable personnellement en cas de non-conformité, c'est le responsable du traitement qui reste seul responsable auprès de l'autorité de contrôle.

Sous-traitant : tiers qui manipule les données pour le compte d'un responsable de traitement. Par exemple, le comptable à qui vous donnez copie des factures clients, ou encore l'hébergeur des données de votre fichier client.

Licéité d'un traitement : ce qui en fonde sa légalité. Un traitement doit reposer sur au moins une base licite mais celles-ci peuvent se cumuler. Six bases de licéité sont reconnues par le RGPD :

- fondée sur le consentement préalable de la personne physique ;
- fondée sur l'exécution d'un contrat avec la personne physique concernée ;
- fondée sur une obligation légale à laquelle le responsable du traitement est soumis ;
- fondée sur la protection des intérêts vitaux de la personne concernée ;
- fondée sur la réalisation d'une mission d'intérêt public ;

- aux fins des intérêts légitimes poursuivis par le responsable du traitement, sauf atteinte aux libertés et droits fondamentaux des personnes.

Consentement : Toute manifestation de volonté libre, éclairée et univoque par laquelle la personne concernée accepte que ses DCP fassent l'objet d'un traitement.

Opt-in : Anglicisme utilisé en communication comme synonyme de consentement donné pour recevoir une newsletter, des SMS…

Opt-out : Anglicisme inverse signifiant que la personne s'est opposée à l'envoi de nouvelles communications.

Principes et droits de la personne

Le RGPD repose sur plusieurs principes généraux :

- Le traitement des données doit être licite.
- Les DCP récoltées sont réduites au minimum nécessaire aux traitements déclarés.
- Le responsable de traitement doit en assurer l'intégrité et la confidentialité.
- La durée de conservation doit être justifiée.
- Les personnes concernées doivent être informées au moment de la collecte des objectifs de celles-ci, et de la façon d'exercer leurs droits.

En effet, les personnes conservent des droits importants sur leurs DCP jusqu'à destruction de celles-ci :

- **Droit d'accès :** les personnes peuvent consulter les DCP les concernant détenues par le tiers.
- **Droit de rectification :** les personnes peuvent en demander la modification.
- **Droit d'effacement :** les personnes peuvent en demander l'effacement.
- **Droit de limitation et d'opposition au traitement :** les personnes peuvent retirer leur accord au traitement des données, totalement ou partiellement.
- **Droit d'opposition au transfert :** les personnes peuvent interdire que leurs données soient transférées à un tiers, et si un tel transfert doit avoir lieu, elles doivent en être préalablement informées.
- **Droit de portabilité :** les personnes peuvent demander à tout moment un export de leur DCP dans un format exploitable par d'autres outils. Cette notion est assez floue actuellement, et peu réaliste au vu de la multiplicité des formats existants et du peu d'interopérabilité des systèmes.

Le droit des personnes semble très étendu, mais il est en réalité limité par les obligations légales : un client peut demander à ce que l'on efface ses données

comptables, mais le professionnel peut s'y opposer parce que la loi le contraint à les garder.

Les obligations pour l'entreprise

Pour une TPE ne traitant pas de données sensibles, les obligations sont assez limitées :

- **Nommer un référent DPO** (c'est plus clair d'un point de vue organisationnel, mais ce n'est pas obligatoire).
- **Tenir un registre des traitements :** il s'agit d'un document qui explicite quelles données sont traitées, dans quels buts et par qui.
- **Sécuriser les données :** le responsable de traitement met en œuvre toutes les mesures nécessaires à la préservation de l'intégrité et de la confidentialité des données. Il récapitule toutes les mesures mise en œuvre dans un document support intitulé "Politique de sécurité des DCP".
- **Informer les personnes :** le responsable de traitement met en place les supports d'information à l'intention des clients pour leur expliquer l'utilisation qui est faite de leurs DCP, les informer de leurs droits et sur la façon de les exercer.
- **Contractualisation avec les sous-traitants :** il s'agit de s'assurer que les sous-traitants mettent en œuvre tous les moyens de sécurisation nécessaires et appliquent eux-mêmes le RGPD.
- **Déclarer les incidents :** si une fuite de données ou autre incident est identifié, le responsable de traitement doit en avertir la CNIL au plus tôt. On verra que cette urgence est relative, suivant le type de données concernées.

Mise en œuvre du RGPD à la clinique

Mettre en place le RGPD au sein de la clinique n'est pas très compliqué. Il faut juste procéder dans l'ordre, sans précipitation. Normalement ce travail ne demande que quelques heures. La période de tolérance instituée par la CNIL permet de ne pas travailler dans l'urgence. Cependant, initier la réflexion est indispensable.

Etape 1 : Cerner les données concernées

Première étape, essentielle pour la suite : quelles données sont récoltées, par qui, qu'en fait-on, que deviennent-elles ? Il s'agit en pratique d'étudier le flux des DCP dans la structure vétérinaire, mais aussi à l'extérieur si celle-ci sont amenées à être traitées par un tiers (et c'est souvent le cas sans qu'on en ait pleinement conscience). Cette analyse permet d'identifier très rapidement les acteurs impliqués dans le traitement des DCP, la localisation de ces données, la totalité des traitements, les points de sécurité importants, les sous-traitants.

Attention, le RGPD ne concerne pas seulement les clients. La plupart des vétérinaires ont également accès aux DCP de leur personnel, ne serait-ce que pour tenir les feuilles de présence ou pour réaliser les bulletins de salaire, ou encore à des DCP de fournisseurs.

Pour garder une vision claire du flux de ces DCP dont les traitements sont sensiblement différents, il est souvent préférable de les étudier séparément.

En pratique :

Le mieux est de représenter le flux de données sur un schéma. Un papier et un crayon suffisent, mais on peut également utiliser des outils informatiques généralistes (Powerpoint par exemple) ou spécialisés. Pour créer le schéma du flux de données, les questions à se poser sont :

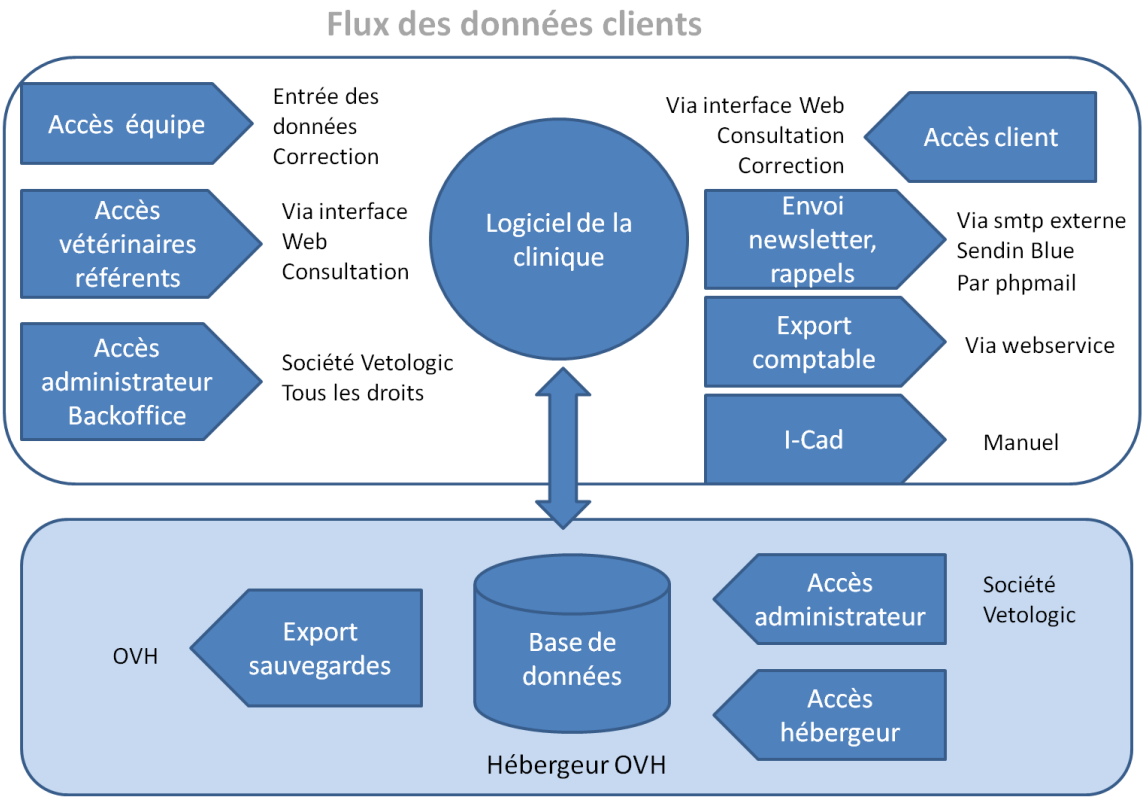
- Comment et par qui sont collectées les données : équipe de la clinique vétérinaire sur l'interface du logiciel de la clinique, site Internet si les clients peuvent créer un compte en ligne ? Autre ?
- Où sont stockées les données ? Dans le logiciel de la clinique certes, mais où ? Localement, sur un serveur installé dans vos locaux ? A distance, chez un prestataire ?
- Qui a accès à ces données ? Le personnel de la clinique ? Les agents de maintenance au sein de vos locaux ? Votre prestataire de logiciel et/ou d'hébergement ? Uniquement quand il vient à la clinique, ou à distance ? Un comptable ?

- Que fait-on de ces données ? Facturation ? Envoi de mails ? De rappels vaccins ? De SMS ? Appels téléphoniques ? Fiches de paie ?
- Lors de leur utilisation, fait-on intervenir un service tiers (SMTP externe, logiciel de mailing local ou en ligne) ? En fait-on des exports ? Si oui, pourquoi et qui en prend connaissance ?
- Si la clinique possède un site Internet avec des comptes clients, comment se fait l'échange entre le logiciel de la clinique et le site ? Y a-t-il plusieurs hébergements ?

Lors de l'analyse du flux de données, il est facile d'oublier un certain nombre de sous-traitants : les hébergeurs, les techniciens qui s'occupent de vos ordinateurs et des systèmes qu'ils font fonctionner, le comptable, les serveurs d'envoi, les serveurs de sauvegarde… Ne pas oublier qu'il faut faire cette analyse pour toutes les DCP, aussi bien les clients que les salariés et associés, ou encore les fournisseurs.

Une clinique aura donc en général au moins deux schémas : données clients, données salariés.

Exemple de schématisation du flux de données client



Etape 2 : Etablir les fiches de traitement

Une fiche de traitement regroupe toutes les informations relatives à un traitement de DCP. Dans les faits, il ne s'agit pas de faire une fiche par traitement (comme par exemple une fiche pour la collecte, une fiche pour l'hébergement, une fiche pour la facturation, une fiche pour l'envoi de mail…). On regroupera dans une même fiche tous les traitements particuliers rattachés à un type de général de traitement. Ainsi une clinique aura classiquement une fiche de traitement clients, une fiche de traitement salariés, et éventuellement une fiche fournisseurs. L'ensemble des fiches de traitement formera le registre de traitement, qui est un document dont l'établissement est obligatoire.

Un modèle de fiche est proposé en annexe I.

FICHE DE REGISTRE DE TRAITEMENT			
N° FDR	FDR001	Nom	
Date de création		Date révision	
Responsable du traitement			
Responsables conjoints			
DPO ou Référent DPO			
Nom des outils			
Traitement hors UE			
SI LE TRAITEMENT EST SOUS TRAITE			
Nom des sous-traitants			
Représentant du ST			
Le contrat précise la finalité du traitement et la catégorie de données			
Le contrat définit les obligations du sous-traitant au regard des droits des personnes			
FINALITES DU TRAITEMENT (Quel est (sont) l'objectif (s) poursuivi (s) ?)			
BASES DE LA LICEITE DU TRAITEMENT (non exclusives)			
• fondé sur le consentement préalable de la personne physique ; • fondé sur l'exécution d'un contrat avec la personne physique concernée ; • fondé sur une obligation légale à laquelle le responsable du traitement est soumis ; • fondé sur la protection des intérêts vitaux de la personne concernée ; • fondé sur la réalisation d'une mission d'intérêt public ; • aux fins des intérêts légitimes poursuivis par le responsable du traitement, sauf atteinte aux libertés et droits fondamentaux des personnes.			
CATEGORIE DE PERSONNES CONCERNEES PAR LE TRAITEMENT			
CATEGORIE DE DONNEES			
DCP	Etat civil, identité, images ? Vie personnelle ? Vie professionnelle ? Economique et financier ? Données de connexion ? Données de localisation ? Internet ? Autres ?		
Sensibilité	NON		
Durée de conservation			
CATEGORIE DES DESTINATAIRES DU TRAITEMENT			

Commentaires par champ :

- Numéro de fiche : numéro de la fiche dans votre registre, 1 pour la première !
- Nom de la fiche : exemple, gestion des clients.
- Date de création et sa date de révision : la fiche est censée être régulièrement révisée, au moins une fois par an.
- Nom du responsable de traitement : le(s) chef(s) d'entreprise.
- Nom du DPO ou du référent DPO s'il a été désigné.
- Nom des outils mis en œuvre (logiciel de la clinique, tableur, logiciels de mailing, d'envoi de SMS…, bref tous les outils utilisés pour le traitement des données).
- Traitement hors Union européenne (oui/non – de préférence on évitera tout traitement hors UE, lequel nécessite une information particulière des clients, la zone hors UE n'étant pas soumise au RGPD).
- Identification des éventuels sous-traitants : hébergeur, comptable, I-Cad, URSSAF, etc.
- Finalités du traitement (à quoi servent les données collectées : objectifs poursuivis facturation, suivi des clients, relances, prospection, présence, fiche de paie…). On n'est pas obligé de tout détailler.
- Base légale du traitement : c'est indispensable. Les bases n'étant pas exclusives, un traitement peut reposer sur plusieurs bases légales. Voir page 3.
- Catégorie des personnes concernées (clients et prospects, salariés, délégués commerciaux…).
- Catégorie des DCP traitées. Il s'agit de donner une vision globale des catégories traitées mais on peut être plus précis. Par exemple, pour le "Autres" : dossiers médicaux des animaux possédés (nom, prénom, adresse, téléphone, mail du propriétaire - nom et identification des animaux, dossiers médicaux des animaux).

  Catégories proposées par la CNIL : **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**.
- Présence de données sensibles : la réponse devrait être toujours non pour une structure vétérinaire !
- Durée de conservation : les données d'un client ne peuvent légalement être utilisées à des fins de prospection que pendant 3 ans après la dernière

transaction. Cependant, la durée de conservation est souvent imposée par d'autres règles : règles comptables, certificats, passeports… D'autre part, dans le cadre de notre activité, effacer le suivi médical d'un animal au bout de 3 ans n'a pas de sens. La mention "Conservation jusqu'à demande de suppression ou obsolescence" est donc justifiée. Pour les documents concernant les salariés, les durées de conservation sont consultables sur https://www.service-public.fr/professionnels-entreprises/vosdroits/F10029.

- Destinataires du traitement : en général interne + éventuelles filiales ou partenaires.

Des champs supplémentaires sont proposés. Ils permettent d'avoir une vision claire sur les mesures mises en œuvre ou à mettre en œuvre pour la gestion des droits des personnes et la protection des DCP. Ne pas hésiter à répondre honnêtement. Comment n'avoir que des "oui" au questionnaire fait l'objet des chapitres suivants !

L'analyse d'impact (PIA)

Lorsque le traitement des données est susceptible d'être à l'origine d'un risque élevé pour les droits et libertés des personnes physiques, une analyse d'impact est obligatoire. Malheureusement, la notion de risque élevé est subjective. En se basant sur les lignes directrices du groupe de travail européen G29 (document mis en avant par la CNIL et consultable en ligne[1]) et dans le cadre de l'activité vétérinaire (en considérant que la clinique ne traite pas de données sensibles), pourraient être soumis à une PIA essentiellement les données évaluatives, comme par exemple la notation des salariés (conséquences personnelles) et l'évaluation des clients (particulièrement des éleveurs, pour lesquels une mauvaise évaluation pourrait avoir des conséquences financières). Mais dans le cadre de la PIA, le RGPD ne fait allusion qu'aux "risques importants sur la vie privée". De plus, le site de la CNIL précise que doivent faire l'objet d'une PIA les traitements remplissant **au moins deux critères** figurant dans la liste suivante : "Evaluation/scoring ; décision automatique avec effet légal ; surveillance systématique ; données sensibles ; données personnelles à large échelle ; croisement de données ; personnes vulnérables ; usage innovant ; exclusion du bénéfice d'un droit ou d'un contrat"[2]. Apparemment, dans le cadre d'un exercice classique de la médecine vétérinaire, aucune analyse d'impact n'est donc nécessaire.

1- *https://www.cnil.fr/sites/default/files/atoms/files/wp248_rev.01_fr.pdf*

2- *https://www.cnil.fr/fr/ce-quil-faut-savoir-sur-lanalyse-dimpact-relative-la-protection-des-donnees-aipd*

Etape 3 : Etablir la politique de sécurité

Le RGPD stipule que le responsable de traitement doit garantir la disponibilité, l'authenticité, l'intégrité et la confidentialité des DCP qu'il détient. Afin de pouvoir démontrer qu'il a pris conscience de ses responsabilités et qu'il a mis en application les mesures techniques et humaines nécessaires, le responsable de traitement tient à la disposition de l'autorité un document récapitulatif appelé "Politique de sécurité". Cette politique contiendra toutes les mesures concernant les DCP, aussi bien celles des clients que des collaborateurs.

Un document-type de politique de sécurité, d'utilisation libre, est proposé (annexe II). Il doit être adapté au cas par cas. Ce document ne doit pas être considéré comme "un papier de plus". Le responsable de traitement s'engage à travers lui à appliquer les mesures décrites, ou à les faire appliquer par ses prestataires.

Remarques particulières :

Paragraphe 3 : formation des utilisateurs

C'est un point important du point de vue sécurité car la plus grande partie des fuites de données se font au travail ou en situation de mobilité, par négligence. Il est donc primordial d'informer et de former ses salariés à la sécurité. A cette fin, des réunions d'équipe seront régulièrement organisées. Plusieurs points seront abordés :

- Confidentialité des données : les données récoltées auprès des clients sont confidentielles, et on ne peut pas les transmettre à d'autres personnes, que ce soit à d'autres clients (personnes à la recherche d'un reproducteur par exemple – sauf accord), ou à des confrères (sauf cas référés avec accord). On peut encore moins les publier sur les réseaux sociaux !
- Seules les personnes autorisées doivent avoir accès aux données. Il ne faut donc pas qu'un client puisse voir la fiche d'un autre client (fiche laissée ouverte au comptoir ou sur le bureau de la salle de consultation). Les accès doivent être protégés par un mot de passe solide, surtout si l'accès est possible à distance, par Internet. Un mot de passe solide est composé d'AU MOINS 8 caractères, et inclut des chiffres, des lettres minuscules, des lettres majuscules, et des signes ($,+,%,*,...). Un mot de passe plus faible peut être cassé par un hacker en quelques minutes.
- La source principale de risque est l'aide-mémoire. Un mot de passe n'a aucune valeur s'il est affiché à côté de l'écran sur un Post-it !
- Les mots de passe sont individuels, sinon un salarié pourrait se connecter au logiciel de la clinique sous une fausse identité, avec une éventuelle intention de nuire.

- Si le personnel est susceptible de se connecter au logiciel de la clinique lors d'un déplacement (visite à domicile, voyage), il doit être averti du risque d'espionnage par un éventuel observateur.

Paragraphe 5.1 : Mesures contre les logiciels malveillants

Les ordinateurs doivent tous être protégés par des antivirus soigneusement mis à jour. Une clef infectée branchée sans mauvaise intention par un stagiaire peut installer dans votre système des chevaux de Troie permettant des effractions, des virus détruisant vos données, ou les codant pour exiger une rançon… C'est d'autant plus important si votre système informatique est relié d'une manière ou d'une autre à Internet. Dans ce cas, la mise en place de pare-feu est recommandée.

Le personnel sera incité à ne pas installer des logiciels d'origine peu sûre, ou à télécharger des mails douteux. Un bon antivirus permet également de se protéger contre cette voie d'infection.

Paragraphe 5.2 : Journalisation des événements

Cela consiste à enregistrer toutes les connexions au système, l'identité de l'utilisateur et éventuellement ses actions. Le but n'est pas d'espionner les membres de l'équipe, mais de pouvoir repérer des opérations anormales et par ce biais, d'identifier d'éventuels piratages de comptes. Les salariés doivent être avertis de ce traçage.

Paragraphe 5.4 : Sauvegarde des informations

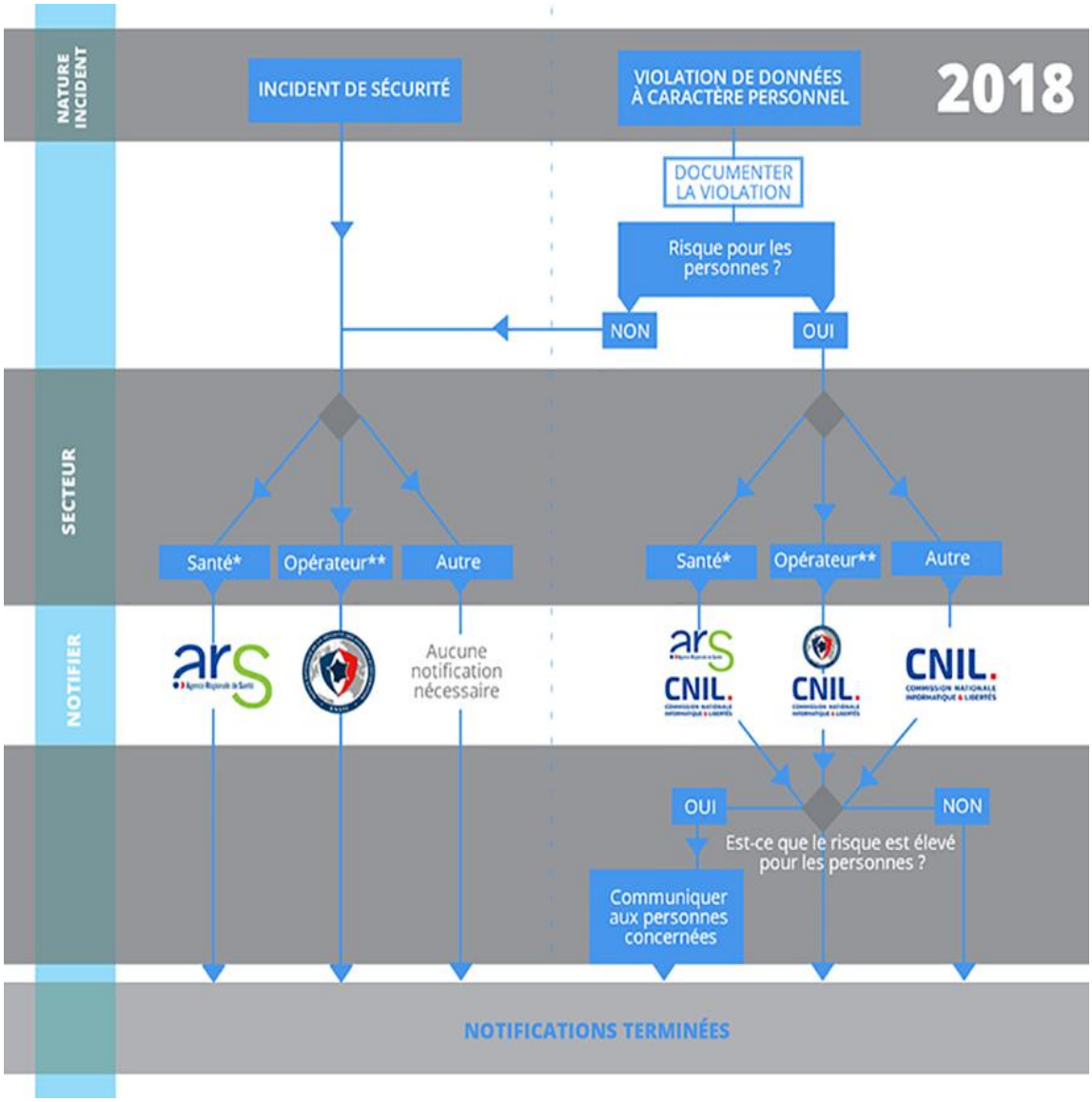
Les sauvegardes doivent être fréquentes (a priori quotidiennes) et régulièrement testées ! Si la qualité des sauvegardes et la possibilité de récupération des données ne sont pas régulièrement évaluées, autant dire qu'elles n'existent pas.

Paragraphe 6.3 : Serveur d'hébergement du système informatique et des données

Normalement, l'analyse préalable du flux de données a permis d'identifier la localisation "physique" des données, mais aussi de leurs sauvegardes. L'hébergement dans le "cloud" ou les sauvegardes à distance sont fréquents (et souhaitables, au moins pour les sauvegardes). Ce n'est pas un problème si les protocoles d'échange sont codés et que l'hébergement est sécurisé, aussi bien en ce qui concerne leur conservation que leur confidentialité. Le responsable de traitement doit cependant s'assurer que le sous-traitant respecte lui-même le RGPD. Dans cet esprit, on évitera les sous-traitants susceptibles de faire transiter les données hors espace européen.

Paragraphe 8 : Gestion des incidents liés à la sécurité de l'information

Tout incident lié aux DCP (perte, fuite) doit censément être signalé le plus rapidement possible à la CNIL. En réalité, cette autorité de contrôle demande au responsable de traitement d'évaluer lui-même s'il y a eu violation, et en cas de réponse positive, d'en estimer les conséquences négatives potentielles pour les victimes. Selon le schéma décisionnel proposé à la CNIL, les violations ne présentant pas de risques pour les personnes et ne concernant pas leur santé ou leur surveillance par des organismes agréés ne sont pas à déclarer.



La clef de la déclaration réside donc dans la quantification du risque pour les personnes. On peut se baser sur le tableau ci-dessous :

NIVEAU	GRAVITE
Maximal	Les personnes concernées pourraient connaître des conséquences significatives, voire irrémédiables, qu'elles pourraient ne pas surmonter.
Important	Les personnes concernées pourraient connaître des conséquences significatives, qu'elles devraient pouvoir surmonter, mais avec des difficultés réelles et significatives.
Limité	Les personnes concernées pourraient connaître des désagréments significatifs qu'elles pourront surmonter malgré quelques difficultés.
Négligeable	Les personnes concernées ne seront pas impactées ou pourraient connaître quelques désagréments, qu'elles surmonteront sans difficultés.

A première vue, une perte ou fuite de données à partir d'une structure vétérinaire n'apparaît générer qu'un niveau de risque négligeable. Cependant, on peut imaginer des cas plus graves : par exemple, fuite de données santé sur les reproducteurs d'un élevage, révélant la présence de tares génétiques…

Quoiqu'il en soit, tout incident, même non déclaré, doit être notifié dans un registre, et les mesures de sécurité nécessaires prises pour éviter une récidive.

Etape 4 : Assurer le respect des droits des personnes

Le RGPD est basé sur le droit fondamental des personnes à la protection de leurs données personnelles. Ceci inclut la licéité du traitement, avec éventuellement obtention préalable du consentement pour la récolte et le traitement des DCP, l'information exhaustive et compréhensible sur leur utilisation, et la possibilité d'exercer les droits de rectification, de suppression et d'opposition par l'individu concerné.

Le consentement préalable

Le consentement préalable est-il obligatoire ?

Non. Pour être légal, et comme vu plus haut, le traitement peut reposer non seulement sur le consentement préalable de la personne physique, mais aussi sur l'exécution d'un contrat avec la personne physique concernée, ou encore sur une obligation légale à laquelle le responsable du traitement est soumis, ou même aux fins des intérêts légitimes poursuivis par le responsable du traitement, sauf atteinte aux libertés et droits fondamentaux des personnes.

Dans la pratique, il n'y a donc pas besoin d'obtenir le consentement des personnes pour récolter des DCP afin d'établir une facturation, une ordonnance, un bulletin de salaire... De plus, la loi autorise d'utiliser les DCP d'un client pour lui proposer des offres de service proches de celles qu'il a déjà souscrite, et ce pendant un délai de 3 ans après l'achat. Les rappels de vaccins ou de suivi s'inscrivent naturellement dans cette ligne (à condition cependant que le client ait été informé – voir plus loin). Ils reposent sur la notion des "intérêts légitimes du responsable de traitement" (attention, cette notion d'intérêt légitime est glissante, il ne faut pas en abuser[4]).

Pour tous les autres traitements, le consentement préalable est nécessaire. Pour une structure vétérinaire, ce peut être l'envoi de newsletter, de publicités par la poste, l'incitation à souscrire des services supplémentaires, ou encore le transfert des données à un tiers, dont par exemple un vétérinaire référent.

La récolte du consentement préalable

Le texte du RGPD n'est pas très cohérent sur ce point. On peut lire à l'article 32 que "*Le consentement devrait être donné par un acte positif clair par lequel la personne concernée manifeste de façon libre, spécifique, éclairée et univoque son accord au traitement des données à caractère personnel la concernant, par exemple au moyen d'une déclaration écrite, y compris par voie électronique, ou d'une déclaration orale.*" Il suffirait donc d'une déclaration orale. Mais à l'article 42, on lit "*Lorsque le traitement est fondé sur le consentement de la personne concernée, le responsable du traitement devrait être en mesure de prouver que ladite personne a consenti à l'opération de traitement.*" *In fine*, le consentement préalable doit donc bien être écrit et conservé. Attention, il est interdit de soumettre la disponibilité d'un service à l'acceptation d'un traitement de DCP, sauf cadre légal (facturation, contrat...).

Le consentement préalable écrit

Il est déjà mis en œuvre par certains commerçants, lesquels vous font signer, en plus d'un bon de commande, une feuille par laquelle vous acceptez ou pas le

traitement de vos DCP. Cette feuille a l'avantage supplémentaire d'apporter au client les informations nécessaires imposées par la loi sur la récolte et le traitement des DCP par l'enseigne.

Le consentement préalable via le site Internet

Si vous disposez d'un site Internet dans lequel les clients ont accès à un espace personnel, il est possible de recueillir le consentement via une case à cocher. C'est le cas classiquement pour les newsletters. Lorsque le client accepte, son adresse IP du moment est enregistrée en base de données, et pourra servir de preuve en cas de besoin. Attention, pour qu'un tel accord soit valable, la case ne doit pas être cochée d'avance, et des informations claires sur le traitement doivent figurer sur la page.

L'information, un point crucial

Le RGPD insiste sur la notion de transparence. Qu'un traitement de DCP soit soumis ou non à consentement préalable, le client doit être informé : informé de la façon dont ses données sont récoltées, informé sur leur usage, informé sur leur éventuel transfert à une tierce partie, que ce soit un sous-traitant ou une autre structure.

Une manière pratique de donner ces informations est de faire figurer un texte dans les conditions générales de fonctionnement qui accompagnent vos factures. Par exemple :

"*Les données personnelles collectées par la clinique des 4 roses sont utilisées afin de gérer au mieux le suivi de vos animaux et d'assurer l'exécution de nos services. Elles pourront, sauf opposition de votre part, être utilisées pour vous alerter sur la nécessité du renouvellement d'un acte médical*".

S'il y a lieu d'être :

"*Vos données personnelles ne seront jamais communiquées à des tiers, sauf agissant pour notre compte dans le cadre d'un traitement spécifique conformément aux finalités pour lesquelles elles ont été recueillies initialement. Ces tiers se sont engagés par contrat à n'utiliser vos données personnelles qu'aux fins convenues.*"

L'information doit aussi porter sur l'exercice des droits. Pour mémoire, l'usager dispose d'un droit d'accès, d'un droit de rectification, d'un droit d'opposition, d'un droit d'effacement, d'un droit de portabilité. Ces droits ne signifient aucunement que votre client a le droit de manipuler sa fiche sur votre ordinateur ! Le droit de consulter, c'est le droit de voir sa fiche, le droit de rectification, c'est le droit de demander de rectifier certaines informations, le droit d'effacement, c'est de demander l'effacement de certains d'entre elles, dans la limite des contraintes

légales et techniques (certaines informations ne pourront pas être effacées – comptabilité, feuilles de paie…). Par contre, la façon d'exercer ces droits doit être précisée : par le biais d'un courrier en recommandé, d'un rendez-vous à la clinique, d'un mail… Attention, il est nécessaire d'informer également les salariés sur la façon d'exercer leurs droits.

Exemple :

"*En application de la législation en vigueur, vous disposez d'un droit d'accès, de rectification, d'effacement, de portabilité, de limitation et d'opposition au traitement de vos données, Vous pouvez exercer ces droits en nous adressant un courrier à Service clients – Clinique vétérinaire des 4 roses – 5 allée Meilland – 50150 La-Roseraie, en précisant vos nom, adresse et numéro de téléphone*."

Il est préférable de désigner une personne de l'équipe chargée de recevoir et traiter ces demandes, et qui en tiendra un cahier de traitement. Il faudra également préalablement définir les protocoles de réponse. Par exemple :

- Demande d'accès : un rendez-vous est pris pour que la personne puisse consulter à l'écran les données qui la concernent, ou une copie papier ou numérique des données lui est envoyée. Si les données figurent dans un site Internet, on s'assure que les utilisateurs peuvent accéder à leur profil.
- Droit de portabilité : en théorie, le client peut demander un export numérique de sa fiche pour la transférer à une autre clinique. En pratique, ce n'est pas à l'ordre du jour, car il n'y a pas officiellement d'interopérabilité. Il est préférable cependant de pouvoir proposer au moins un export de ces données en format numérique, bien que le format reste à déterminer (XML, autre ?).
- Demande de modifications : la personne est contactée par téléphone ou rencontrée à la clinique, ou il lui est demandé d'envoyer un courrier précisant les modifications. Les modifications demandées sont apportées, si elles ne sont pas contraires aux obligations légales. Sur un site Internet, les utilisateurs ont en général la possibilité de modifier tout ou partie de leurs données.
- Demande de suppression : cette demande s'arrête aux contraintes légales. Un certain nombre de données peuvent être supprimées de la fiche (téléphone, adresse mail, données santé des animaux), mais ce droit est limité à ce qui n'est pas nécessaire et obligatoire à la tenue de la comptabilité ou des certificats santé ou vaccination par exemple. Ainsi, en fonction du système informatique, il sera possible ou pas de supprimer certaines données, en faisant un distinguo entre "données courantes", dont on se sert régulièrement, et "données archivées", rangées ailleurs, avec une protection supplémentaire. Enfin, ne pas oublier que les données d'un client ne peuvent faire l'objet d'un traitement de prospection 3 ans après la dernière transaction. Même si on ne peut pas les effacer pour des raisons techniques ou réglementaires, il n'est pas autorisé de s'en servir.

- Opposition au traitement : la signification de l'usager de son opposition au traitement (sauf traitement obligatoire de par la loi) doit pouvoir être inscrite dans sa fiche et prise en compte lors du traitement. Si un client s'oppose à ce que vous utilisiez son adresse mail, vous n'avez tout simplement pas le droit de le faire, quelle qu'en soit la raison. La plupart du temps, l'opposition se réfère à la communication, et les règles de bases sont rappelées plus loin. Le client doit pouvoir aussi s'opposer au transfert de ses données (à un vétérinaire référent, à une autre entreprise…). Son droit doit pouvoir s'exercer immédiatement, il doit donc être informé très clairement d'une telle possibilité de transfert et du fait qu'il peut s'y opposer.

Quelques rappels de droit de la communication

- Vous pouvez envoyer un SMS, un mail ou une lettre à un client ayant souscrit à un service depuis moins de trois ans si celui-ci ne s'y est pas opposé, qu'il a été informé du pourquoi de la récolte de ses coordonnées, et que la communication concerne ce service ou un service similaire.
- Vous ne pouvez pas envoyer un SMS ou un mail à un individu non client (donc un prospect) si la personne n'a pas donné clairement son consentement.
- Tout SMS ou mail envoyé doit comprendre un lien permettant de s'opposer immédiatement et facilement aux prochains envois (mention Stop pour les SMS, lien de désinscription pour les mails).
- Une personne doit pouvoir s'opposer à la réception de courriers postaux de votre part.

Les supports

L'ensemble de ces considérations montrent la nécessité de disposer de supports pour informer les clients. Voici quelques propositions :

Support d'information général

Ce peut être une feuille volante distribuée à chaque client, une affiche bien visible en salle d'attente ou au comptoir, ou mieux un texte intégré aux conditions générales de fonctionnement, accompagnant chaque facture.

Exemple :

"*Les données personnelles collectées par la clinique des 4 roses sont utilisées afin de gérer au mieux le suivi de vos animaux et d'assurer l'exécution de nos services. Nous ne collectons que les données indispensables à la gestion optimale de notre relation. Vos coordonnées pourront, sauf opposition de votre part, être utilisées pour vous alerter sur la nécessité du renouvellement d'un acte médical*.

Vos données personnelles ne seront jamais communiquées à des tiers, sauf agissant pour notre compte dans le cadre d'un traitement spécifique conformément aux finalités pour lesquelles elles ont été recueillies initialement. Ces tiers se sont engagés par contrat à n'utiliser vos données personnelles qu'aux fins convenues.

Pour assurer le meilleur suivi de la santé de votre animal, les données le concernant sont conservées a minima toute sa vie, sauf demande d'effacement de votre part.

En application de la législation en vigueur, vous disposez d'un droit d'accès, de rectification, d'effacement, de portabilité, de limitation et d'opposition au traitement de vos données. Vous pouvez exercer ces droits en nous adressant un courrier à Service clients – Clinique vétérinaire des 4 roses – 5 allée Meilland – 50150 La-Roseraie, en précisant vos nom, adresse et numéro de téléphone."

Politique de gestion des données pour le site Internet

Il s'agit d'un document récapitulant le cadre du traitement des DCP via votre site Internet. Un lien, en général en bas de page, renvoie vers cette politique. Attention, la mise à disposition de ce document sur votre site Internet ne remplace pas l'obligation d'une information claire et concise lors du remplissage en ligne d'un formulaire par un client, elle la complète.

Ainsi, sur l'interface de la création d'un compte, on pourra afficher :

" *Les informations demandées ci-dessous (nom, prénom, adresse mail…) sont utilisées afin de permettre votre connexion au site et de gérer au mieux l'exécution de nos services et le suivi de vos animaux. Notre politique de protection des données personnelles est consultable en cliquant ici.*"

et renvoyer à la politique générale dont une proposition de contenu est donné en annexe III.

Une information supplémentaire doit être affichée lorsqu'on propose une inscription à une newsletter ou l'envoi de SMS :

" *En cochant cette case, j'accepte de recevoir la newsletter de la clinique. Je serais ainsi tenu au courant des services proposés et des nouveautés. Je pourrais me désinscrire à tout moment.*

En cochant cette case, j'accepte de recevoir des SMS de la clinique. Ces SMS me permettront de recevoir les rappels de vaccination. Je pourrai me désinscrire à tout moment."

Demande de consentement préalable

C'est un document à faire signer et à archiver à chaque fois que cela est nécessaire, par exemple :

- lorsque les données vont être envoyées à un tiers ;
- pour l'inscription à l'envoi de SMS et/ou newsletters hors services déjà souscrits (sauf si l'opt-in est récolté via le site Internet) ;
- pour la création d'une fiche de prospect (la personne n'est pas encore cliente).

Exemples :

" *Le cas de votre animal nécessitant l'intervention d'un spécialiste, vous acceptez par la présente que vos données personnelles et le dossier de votre animal soit transféré au Dr. xxxx, adresse.* "

" *Afin de vous permettre d'être informé sur les services et nouveautés proposés par la clinique des 4 roses, vous acceptez de recevoir des informations de notre part - par mail - par SMS – par courrier. Vous pourrez vous désinscrire tout moment.*"

Etape 5 : les sous-traitants

L'analyse du flux de données permet d'identifier les différents sous-traitants impliqués. Le responsable de traitement a l'obligation de s'assurer que les sous-traitants prennent leurs responsabilités vis-à-vis des DCP qui leur sont confiées. Cette assurance est l'objet d'une contractualisation. Le contrat doit permettre d'éclairer les points suivants :

- Engagement du sous-traitant à respecter les règles du RGPD.
- Engament du sous-traitant à faire respecter ces règles par ses éventuels propres sous-traitants.
- Engagement du sous-traitant à prévenir le responsable de traitement en cas de violation des données.
- Lors du sous-traitement, y a-t-il transfert des données à l'étranger, hors espace européen ? Si c'est le cas, les propriétaires des DCP doivent en être informés. Le mieux est d'éviter cette situation.

Un exemple de contrat de sous-traitance est proposé en annexe IV.

Faut-il réellement passer un contrat spécifique de sous-traitance avec chaque opérateur ? En théorie oui, en pratique, ce n'est pas possible. Par exemple, on ne voit pas un organisme comme I-Cad passer un contrat avec chaque identificateur. Ou encore OVH, célèbre société d'hébergement informatique en faire de même avec chaque propriétaire de base de données hébergées. Ces grands prestataires

ont en général publié une politique de protection des données commune à tous leurs clients. Collecter et archiver ces politiques pour pouvoir montrer le cas échéant aux autorités de contrôle qu'on s'est préoccupé de ce que font nos sous-traitants des données que nous leur transmettons devrait suffire à nous couvrir.

Etape 6 : Mettre en œuvre !

L'établissement des documents de support de la politique de protection des données est le pivot de sa mise en œuvre, mais elle n'en est pas le seul élément. Elle permet d'identifier les actions physiques à mener pour qu'elle soit effective, comme :

- la désignation d'un responsable, le référent DPO, acteur central de l'application du RGPD, et d'un référent sécurité, responsable des sauvegardes, protections et mises à jour ;
- la formation de l'équipe aux règles de sécurisation des données, décrites dans la politique de protection (protection des accès, des mots de passe, du matériel, des canaux d'échange) ;
- l'adaptation des outils informatiques (modification du site Internet, du logiciel de gestion de la clinique, du logiciel comptable…) ;
- la prise en compte des normes RGPD dans l'acquisition ou le développement de nouveaux outils.

Un plan de mise en œuvre du RGPD pourrait être le suivant :

1) Désignation d'un responsable. Mise à disposition de moyens : du temps essentiellement.
2) Analyse du flux de données, qui permet d'identifier les données concernées et leurs localisations, les acteurs, les accès.
3) Création des fiches de traitement, ce qui permet de mettre en évidence les faiblesses de la situation en cours.
4) Rédaction de la politique de sécurité, énumérant l'ensemble des mesures nécessaires pour assurer l'intégrité et l'inviolabilité des DCP.
5) Mise en place de ces mesures, nécessitant éventuellement des modifications logicielles, ou des archivages papier sécurisés. Formation de l'équipe à la sécurité, lors d'une réunion dédiée.
6) Mise à jour des fiches de traitement.
7) Rédaction de la politique de gestion des données.
8) Intégration de cette politique dans les conditions générales de fonctionnement, dans le site Internet.
9) Ecriture des protocoles d'information des personnes et de la récolte du consentement préalable. Formation de l'équipe lors d'une réunion dédiée.

10) Mise à jour des fiches de traitement.

11) Vérification des conditions générales de fonctionnement des sous-traitants et contractualisation. Archivage des contrats.

12) Mise à jour des fiches de traitement.

Ensuite, le dossier est repris régulièrement, tous les ans par exemple, pour s'assurer que les règles de sécurité sont bien respectées, les rappeler si nécessaire, surtout si l'équipe a changé. Une réunion annuelle de sensibilisation au RGPD est préconisée. Les modifications des objectifs de traitement et des flux sont surveillées, et les fiches de traitement modifiées. En cas d'intervention de nouveaux sous-traitants, les clauses RGPD sont intégrées d'office dans le contrat.

Tout cela peut sembler chronophage, mais en réalité, une fois les documents et protocoles élaborés (ce qui, dans le cadre d'une activité vétérinaire, et en se reposant sur les documents fournis ici devrait prendre une dizaine d'heures), cela n'est plus une question de temps mais une question d'esprit. Inculquer le respect des données personnelles à l'équipe ne devrait pas être trop difficile, car si nous sommes des prestataires de service, nous sommes aussi des usagers. Nous n'aimons pas que nos données personnelles soient divulguées à tout vent, nous voulons en garder le contrôle. Nos clients aussi, tout simplement.

Sources :

1. CNIL : Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 (2018). https://www.cnil.fr/fr/reglement-europeen-protection-donnees Consulté août 2018.
2. CNIL : RGPD : passer à l'action. https://www.cnil.fr/fr/rgpd-passer-a-laction Consulté août 2018
3. CNIL : RGPD en pratique : maîtrisez votre relation client. https://www.cnil.fr/fr/rgpd-en-pratique-maitrisez-votre-relation-client Consulté août 2018.
4. Ledieu-Avocats : RGPD-GDPR —> les traitements SANS consentement « nécessaires aux intérêts légitimes » (2017). https://www.ledieu-avocats.fr/gdpr-interets-legitimes/ Consulté août 2018
5. Foucault J. : RGPD Apprendre à mettre en œuvre le système de gestion de la protection des données personnelles. Support de cours ENI services, 2018.

Annexe I : Fiche de traitement

FICHE DE REGISTRE DE TRAITEMENT			
N° FDR	**FDR001**	Nom	
Date de création		Date révision	
Responsable du traitement			
Responsables conjoints			
DPO ou Référent DPO			
Nom des outils			
Traitement hors UE			
SI LE TRAITEMENT EST SOUS TRAITE			
Nom des sous-traitants			
Représentant du ST			
Le contrat précise la finalité du traitement et la catégorie de données			
Le contrat définit les obligations du sous-traitant au regard des droits des personnes			
FINALITES DU TRAITEMENT (Quel est (sont) l'objectif (s) poursuivi (s) ?)			
BASES DE LA LICEITE DU TRAITEMENT (non exclusives)			
• fondé sur le consentement préalable de la personne physique ; • fondé sur l'exécution d'un contrat avec la personne physique concernée ; • fondé sur une obligation légale à laquelle le responsable du traitement est soumis ; • fondé sur la protection des intérêts vitaux de la personne concernée ; • fondé sur la réalisation d'une mission d'intérêt public ; • aux fins des intérêts légitimes poursuivis par le responsable du traitement, sauf atteinte aux libertés et droits fondamentaux des personnes.			

CATEGORIE DE PERSONNES CONCERNEES PAR LE TRAITEMENT	
CATEGORIE DE DONNEES	
DCP	Etat civil, identité, images ? Vie personnelle ? Vie professionnelle ? Economique et financier ? Données de connexion ? Données de localisation ? Internet ? Autres ?
Sensibilité	
Durée de conservation	
CATEGORIE DES DESTINATAIRES DU TRAITEMENT	

GESTION DES DROITS ET PRINCIPES ATTACHES AUX PERSONNES CONCERNEES	
Le traitement est licite, sa finalité est déterminée, explicite et légitime (Art 6)	
Les données collectées sont réduites au minimum nécessaire (Art 47)	
L'intégrité et la confidentialité des données sont garanties (Art 32)	
La durée de conservation est justifiée au regard de la finalité (Art 13)	
L'information est concise pour l'exercice des droits de la personne (Art 13)	
Droit d'accès aux données (Art 15)	
Droit de rectification des données (Art 16)	
Droit d'effacement des données (Art 17)	

Droit de limitation du traitement (Art 18)	
Droit de portabilité des données (Art 20)	
Droit d'opposition au traitement (Art 21)	
Droit d'opposition au transfert de données (Art 46)	
EXEMPLE DE MESURES DE PROTECTION DES DONNEES Disponibilité, Intégrité, Confidentialité	
L'accès physique aux locaux contenant des équipements numériques DCP	
Les actifs numériques traitant de DCP sont protégés contre les malwares et les attaques logiques	
Les utilisateurs en situation de mobilité sont sensibilisés au vol et à l'écoute et observation passive	
Les données sont sauvegardées et des tests de restauration effectués	
Les utilisateurs sont formés aux outils et vigilants dans leurs usages et leurs manipulation	
Les gestionnaires de droits d'accès aux outils et aux DCP sont formellement identifiés	
L'extraction et l'export de DCP sont contrôlés	
Les services en ligne, les échanges ou transferts sur les réseaux sont protégés contre l'interception	
La gestion des flux de données est cartographiée pour contrôler les transferts ou traitements hors UE	
PIA - «susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques».	
Avis DPO :	

Annexe II
Politique de sécurité des données à caractères personnelles

mise à jour le ….

Objet

Le règlement (UE) 2016/679 du parlement européen et du conseil du 27 avril 2016 impose que les organismes mettant en œuvre des traitements ou disposant de fichiers de données en garantissent la sécurité. Par sécurité des données, on entend l'ensemble des « précautions utiles, au regard de la nature des données et des risques présentés par le traitement », pour notamment, « empêcher que les données soient déformées, endommagées, ou que des tiers non autorisés y aient accès ».

Organisation de la sécurité

Le référent sécurité est …… (nom et coordonnées du référent s'il y en a un, sinon le chef d'entreprise).

La clinique vétérinaire …… s'engage à fournir les ressources pour faire appliquer la présente politique. La politique de sécurité est révisée régulièrement.

Formation des utilisateurs

Les utilisateurs des systèmes d'information sont formés à :

- l'importance de la sécurisation des DCP ;
- les règles de sécurisation des mots de passe ;
- les risques d'accès aux données par des tiers, particulièrement en situation de mobilité : vol de matériel, discrétion dans les lieux publics et au bureau ;
- l'importance des antivirus.

(Le cas échéant si un système d'enregistrement des connexions sur le logiciel de la clinique a été mis en place, ce qui est souvent le cas, même si on ne vous l'a pas dit. Se renseigner auprès de votre fournisseur.) -> De plus, les utilisateurs ont été

informés de l'enregistrement de leurs interventions dans un fichier log (ou dans la base de données).

Les personnes accédant au système d'information en situation de mobilité sont sensibilisées aux bonnes pratiques pour éviter le vol de matériel et d'identifiants dans les lieux publics et les transports (observation passive, écoute passive).

Cryptographie

Le système informatique, le site de la clinique utilisent pour eux-mêmes et pour les échanges entre eux un protocole sécurisé et chiffré HTTPS.

Sécurité liée à l'exploitation

Mesures contre les logiciels malveillants

Chaque poste informatique fixe ou mobile appartenant à la clinique est doté d'un antivirus performant et à jour. Le responsable de l'installation et du maintien à jour des antivirus de chaque poste, fixe ou portable, est ..... (un membre de l'équipe ou un prestataire).

Le réseau Internet de la clinique est protégé par une clef sécurisée et un pare-feu, régulièrement mis à jour par ..... (un membre de l'équipe ou un prestataire).

Journalisation des événements

Les connections système informatique de la clinique sont mémorisées dans un fichier log.

Sauvegarde des informations

Une sauvegarde régulière des bases de données du système informatique (et de la base de données des salariés) est effectuée (de telle manière, tous les tant).

La fiabilité des sauvegardes est testée régulièrement (de telle façon). Les sauvegardes sont protégées (de telle façon).

Contrôle d'accès

Système informatique de la clinique

Accès vétérinaires et ASV

Par cet accès les utilisateurs peuvent entrer et modifier les DCP des clients et des contacts laboratoires. La sécurité est assurée par mot de passe individuel, composé

d'au moins 8 caractères, et comportant des chiffres, des lettres et des signes. Les mots de passe, personnels, ne sont connus que du seul utilisateur (*si c'est le cas* : ainsi que du responsable sécurité). Les mots de passe sont renouvelés tous les ……..

Accès administrateurs

Les administrateurs ont accès à une interface de gestion du logiciel. La liste des utilisateurs autorisés est limitée et établie :

- M. ….., vétérinaire associé
- Mme ……, société ……., prestataire

Ces personnes s'engagent à utiliser un mot de passe secret et hautement sécurisé.

Accès Logiciel de gestion des salariés

L'accès à ce logiciel est réservé à des utilisateurs clairement identifiés :

- Mme ……, vétérinaire associée
- M. ….., comptable

La sécurisation est assurée (de telle façon).

Eventuellement : Les connexions au site sont enregistrées dans la base de données – dans un fichier log.

Archives bulletin de salaires

Les bulletins de salaire sont conservés pendant la durée légale sous (tel) format. Les archives sont conservées (en tel lieu) (sous tel format). L'accès à ces archives est réservé à des utilisateurs clairement identifiés :

- Mme ……, vétérinaire associée
- M. ….., vétérinaire associé

La sécurisation est assurée (de telle façon : archive numérique protégée par mot de passe, bureau fermé à clef…).

Serveur d'hébergement du système informatique

L'hébergement des données est effectué par la société xxxxxxx qui en gère la sécurité et les accès.

OU

Les données sont hébergées sur un serveur local, situé au sein de la clinique. Les personnes ayant accès au serveur sont :

- M. ....., prestataire de service de la société .....

La société ..... s'est engagée par contrat à respecter toutes les règles de sécurité requises pour assurer la pérennité et la confidentialité des données à caractère personnel hébergées par ses soins (ou sur le serveur de la clinique), et à faire respecter ces règles par tout sous-traitant auquel elle pourrait faire appel. Le contrat est joint à la présente politique.

Sous-traitants

Les sous-traitants identifiés sont :

- la société x pour l'hébergement des données ;
- la société y pour la maintenance du matériel informatique ;
- la société z pour la maintenance du logiciel de la clinique ;
- la société w pour l'envoi des lettres de relances ;
- la société k pour l'édition des bulletins de salaires ;
- la médecine du travail ;
- l'expert comptable, le commissaire au compte ...

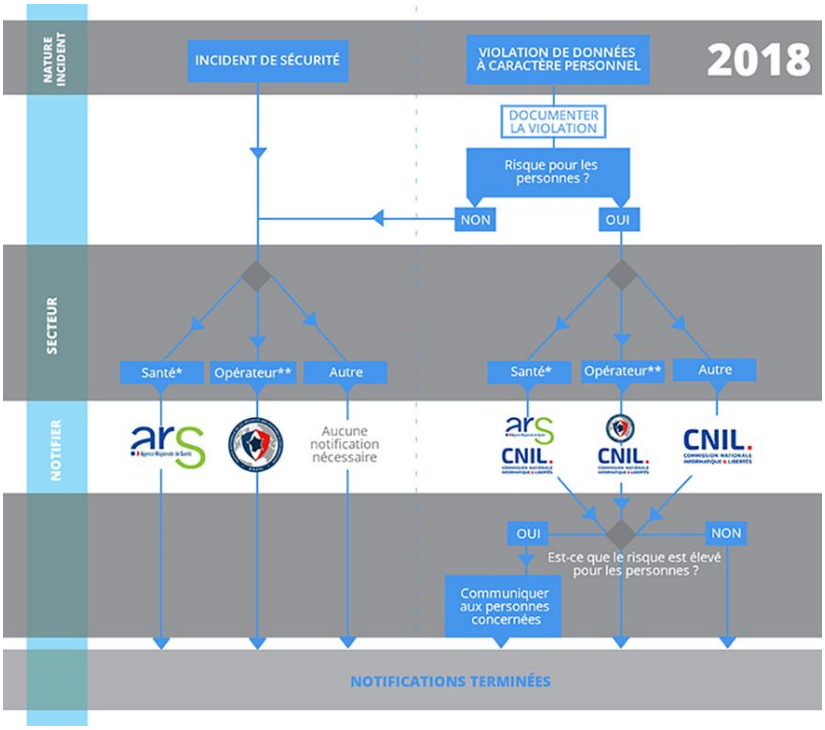
La récolte des politiques de sécurité et de protection des DCP de chacune de ces sociétés a été effectuée. Elles sont jointes au présent document.

Gestion des incidents liés à la sécurité de l'information

Toute personne salariée ou non de la clinique constatant des activités anormales, des tentatives de connexion suspecte, ou une violation des DCP la signale le plus rapidement possible au responsable sécurité nommé dans le présent document.

Une évaluation de l'incident est effectuée par le responsable sécurité, afin de déterminer s'il y a eu ou non violation de DCP, et de contrôler la qualité de la sécurisation.

L'incident est qualifié suivant l'arbre décisionnel proposé par la CNIL, afin de décider ou non d'une déclaration à la CNIL.



** Établissements de santé, hôpitaux des armées, laboratoires de biologie médicale et centres de radiothérapie*

*** Opérateur d'importance vitale (OIV), opérateur de service essentiel (OSE) ou opérateur de service numérique (OSN) mettant à disposition des places de marché et les moteurs de recherche en ligne et des services d'informatique en nuage, service de confiance (SDC), ou opérateurs Télécom*

Si une notification est nécessaire, elle est faite en ligne sur le site de la CNIL (outil non opérationnel à ce jour). Les personnes dont les DCP sont concernées et qui pourraient être exposées à un risque élevé* seront alors averties.

Tous les incidents sont documentés sur un registre.

** A priori, aucune DCP détenue par la clinique vétérinaire ne présente un risque élevé pour les personnes.*

ANNEXE III
Politique de protection des données personnelles

La présente politique de protection des données personnelles décrit les méthodes appliquées pour recueillir, gérer et utiliser les données personnelles. Cette politique peut être modifiée, complétée, supprimée ou mise à jour ; cependant, nous traiterons toujours vos informations personnelles conformément à la politique en vigueur au moment de leur collecte.

Notre objectif est de vous faire part régulièrement sur cette page des modifications éventuelles apportées à cette politique, afin que vous soyez toujours pleinement informé des catégories d'informations que nous recueillons, de la manière dont nous les utilisons, et des circonstances dans lesquelles elles peuvent être communiquées. Notre politique de protection des données est accessible à partir de toutes les pages du site.

Garanties sur la confidentialité des données

Le terme "données personnelles", tel qu'il est utilisé dans la présente politique, fait référence aux informations suivantes : vos nom et prénom, votre adresse postale et mail, votre numéro de téléphone, données permettant de vous identifier sur le site et de gérer le dossier de vos animaux. En règle générale, nous traiterons vos données personnelles selon la procédure décrite dans cette politique. Nous nous réservons le droit de procéder à des traitements supplémentaires qui seraient requis par la loi.

Utilisation des données personnelles

L'accès à la partie privée du site clinique-4-roses.com est réservé aux personnes inscrites sur le site. Des éléments permettant cette identification vous sont demandés, ainsi que les éléments permettant de vous créer un compte utilisateur. Selon la réglementation en vigueur, vos données personnelles nous permettent de vous fournir des services ou de communiquer avec vous selon votre choix d'abonnement à nos lettres électroniques.

Non-communication des données personnelles

Vos données personnelles ne seront jamais vendues, ni partagées ou communiquées à des tiers, sauf agissant pour notre compte dans le cadre d'un traitement spécifique conformément aux finalités pour lesquelles elles ont été recueillies initialement. Ces tiers se sont engagés par contrat à n'utiliser vos données personnelles qu'aux fins convenues, et à ne pas les vendre ou divulguer à d'autres tiers sauf si la loi le requiert.

Par ailleurs, les données personnelles pourront être divulguées à un tiers si nous y sommes contraints dans le cadre d'une loi en ou d'une disposition réglementaire en vigueur, d'une ordonnance judiciaire ou d'une réglementation gouvernementale, ou si cette divulgation est nécessaire dans le cadre d'une enquête, ou d'une procédure pénale, sur le territoire national ou à l'étranger.

Droit d'accès, de rectification et d'opposition

Vous disposez d'un droit d'accès et un droit d'opposition au traitement de vos données personnelles pour des raisons légitimes, c'est-à-dire si ce traitement n'est pas raisonnablement nécessaire à la poursuite de notre intérêt légitime tel que décrit dans la présente politique, ou au respect de la loi. Vous avez accès à vos données personnels une fois connecté au site, et vous pouvez les modifier (menu "Mon profil"). Si vous souhaitez effacer votre compte et vos données, ou encore vous opposez à leur traitement, merci d'envoyer via le formulaire disponible sur la page https://clinique-4-roses/nous-contacter.html.

Sécurité et confidentialité

Pour assurer la sécurité et la confidentialité des données personnelles que nous recueillons en ligne, nous utilisons des accès protégés par des dispositifs standards tels que pare-feu et mot de passe. Lors du traitement de vos données personnelles, nous prenons toutes les mesures raisonnables visant à les protéger contre toute perte, utilisation détournée, accès non autorisé, divulgation, altération ou destruction.

Cookies

Un "cookie" est un petit fichier d'information envoyé sur votre navigateur et enregistré au sein de votre terminal (ex : ordinateur, smartphone). Nous n'utilisons que des cookies fonctionnels vous permettant d'utiliser le site en tant que personne autorisée, ainsi que des informations générales de navigation afin de statistiques. Nous ne recueillons pas d'information personnalisée concernant votre visite de ce site.

Comment nous contacter

Si vous avez des questions ou des réclamations concernant notre respect de la présente politique de confidentialité des données, ou si vous souhaitez nous faire part de recommandations ou des commentaires visant à améliorer sa qualité, contactez-nous via le formulaire disponible sur la page https://clinique-4-roses/nous-contacter.html.

ANNEXE IV
Contrat de sous-traitance des données à caractère personnel

Entre

la clinique vétérinaire ..... représentée par .....
ci-après "le responsable de traitement", d'une part,

et

la société .....
ci-après "le sous-traitant", d'autre part,

Objet

Les présentes clauses ont pour objet de définir les conditions dans lesquelles le sous-traitant s'engage à effectuer pour le compte du responsable de traitement les opérations de traitement de données à caractère personnel définies ci-après.

Dans le cadre de leurs relations contractuelles, les parties s'engagent à respecter la réglementation en vigueur applicable au traitement de données à caractère personnel et, en particulier, le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 applicable à compter du 25 mai 2018 (ci-après, « le règlement européen sur la protection des données »).

Description du traitement faisant l'objet de la sous-traitance

Le sous-traitant est autorisé à traiter pour le compte du responsable de traitement les données à caractère personnel nécessaires pour fournir les services suivants : ..... Les données à caractère personnel traitées sont : .....

Les catégories de personnes concernées sont : les clients, prospects, salariés et fournisseurs du responsable de traitement.

Pour l'exécution du service objet du présent contrat, le responsable de traitement met à la disposition du sous-traitant un accès à .....

Durée du contrat

Le présent contrat entre en vigueur à compter du ..... et durera tant que le sous-traitant sera en charge des services décrits ci-dessus.

Obligations du sous-traitant vis-à-vis du responsable de traitement

Le sous-traitant s'engage à :

- à respecter les obligations imposées par le règlement européen sur la protection des données ;
- à ne pas procéder à un quelconque traitement hors de la Communauté européenne.
- traiter les données uniquement pour la ou les seule(s) finalité(s) qui fait/font l'objet de la sous-traitance ;
- garantir la confidentialité des données à caractère personnel traitées dans le cadre du présent contrat ;
- veiller à ce que les personnes autorisées à traiter les données à caractère personnel en vertu du présent contrat s'engagent à respecter la confidentialité ou soient soumises à une obligation légale appropriée de confidentialité ; reçoivent la formation nécessaire en matière de protection des données à caractère personnel.

Sous-traitance : Le sous-traitant peut faire appel à un autre sous-traitant (ci-après, « le sous-traitant ultérieur ») pour mener des activités de traitement spécifiques. Dans ce cas, il informe préalablement et par écrit le responsable de traitement de tout changement envisagé concernant l'ajout ou le remplacement d'autres sous-traitants. Cette information doit indiquer clairement les activités de traitement sous-traitées, l'identité et les coordonnées du sous-traitant et les dates du contrat de sous-traitance. Le responsable de traitement dispose d'un délai minimum de 1 mois à compter de la date de réception de cette information pour présenter ses objections. Cette sous-traitance ne peut être effectuée que si le responsable de traitement n'a pas émis d'objection pendant le délai convenu.

En cas de recrutement d'autres sous-traitants ultérieurs, le sous-traitant doit recueillir l'autorisation écrite, préalable et spécifique du responsable de traitement.

Le sous-traitant ultérieur est tenu de respecter les obligations du présent contrat pour le compte et selon les instructions du responsable de traitement. Il appartient au sous-traitant initial de s'assurer que le sous-traitant ultérieur présente les mêmes garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles appropriées de manière à ce que le traitement réponde aux exigences du règlement européen sur la protection des données. Si le sous-traitant ultérieur ne remplit pas ses obligations en matière de protection des données, le sous-traitant initial demeure pleinement responsable devant le responsable de traitement de l'exécution par l'autre sous-traitant de ses obligations.

Droit d'information des personnes concernées

Il appartient au responsable de traitement de fournir l'information aux personnes concernées par les opérations de traitement au moment de la collecte des données.

Notification des violations de données à caractère personnel

Le sous-traitant notifie au responsable de traitement toute violation de données à caractère personnel dans un délai maximum de 48 heures après en avoir pris connaissance et par le moyen suivant : courrier électronique et téléphone. 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

Mesures de sécurité

Le sous-traitant s'engage à mettre en œuvre les mesures de sécurité suivantes :

.....

Sort des données

Au terme de la prestation de services relatifs au traitement de ces données, le sous-traitant s'engage, au choix du responsable de traitement à détruire toutes les données à caractère personnel ou à renvoyer toutes les données à caractère personnel au responsable de traitement ou à renvoyer les données à caractère personnel au sous-traitant désigné par le responsable de traitement.

Le renvoi doit s'accompagner de la destruction de toutes les copies existantes dans les systèmes d'information du sous-traitant. Une fois détruites, le sous-traitant doit justifier par écrit de la destruction

Délégué à la protection des données

Le sous-traitant communique au responsable de traitement le nom et les coordonnées de son délégué à la protection des données, s'il en a désigné un conformément à l'article 37 du règlement européen sur la protection des données.

Registre des catégories d'activités de traitement

Le sous-traitant déclare tenir par écrit un registre de toutes les catégories d'activités de traitement effectuées pour le compte du responsable de traitement comprenant :

- le nom et les coordonnées du responsable de traitement pour le compte duquel il agit, des éventuels sous-traitants et, le cas échéant, du délégué à la protection des données ;
- les catégories de traitements effectués pour le compte du responsable du traitement ;
- le cas échéant, les transferts de données à caractère personnel vers un pays tiers ou à une organisation internationale, y compris l'identification de ce pays tiers ou de cette organisation internationale et, dans le cas des transferts visés à l'article 49, paragraphe 1, deuxième alinéa du règlement européen sur la protection des données, les documents attestant de l'existence de garanties appropriées ;
- dans la mesure du possible, une description générale des mesures de sécurité techniques et organisationnelles ;
- des moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement ;
- des moyens permettant de rétablir la disponibilité des données à caractère personnel et l'accès à celles-ci dans des délais appropriés en cas d'incident physique ou technique ;
- une procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement.

Documentation

Le sous-traitant met à la disposition du responsable de traitement la documentation nécessaire pour démontrer le respect de toutes ses obligations.

Obligations du responsable de traitement vis-à-vis du sous-traitant

Le responsable de traitement s'engage à :

- fournir au sous-traitant l'accès aux données visées au II des présentes clauses ;

- veiller, au préalable et pendant toute la durée du traitement, au respect des obligations prévues par le règlement européen sur la protection des données de la part du sous-traitant.

Fait à …… le ……

Le responsable de traitement Le sous-traitant