WilhelmGilliéron
AVOCATS

Auteur: Wilhelm Avocats | Le : 4 octobre 2021

Protection des données et professions libérales : pas si compliqué

Le 10 juin 2021, l'autorité italienne en matière de protection des données condamnait un dentiste à une amende de € 20'000, motif étant tiré du fait que le dentiste avait refusé de traiter un patient atteint du virus HIV sans avoir clairement énoncé le fait qu'une telle divulgation pouvait entraîner un refus de traitement, et non pas seulement des conséquences quant au possible traitement.

Si le cas est particulier, il coupe court à toute croyance suivant laquelle la conformité en matière de protection des données ne concernerait que les grosses sociétés, seule à même d'exploiter de manière massive des données personnelles et donc seules à être dans le collimateur des autorités et de possibles sanctions.

Se pose dès lors la question de savoir quelles mesures les médecins, dentistes et autres avocats (que je qualifierais ensuite par souci de simplification par le terme de « praticien ») devraient raisonnablement mettre en œuvre pour éviter toute mésaventure.

A. *Pas d'application du RGPD*

En réalité, ces démarches sont assez simples. Rappelons tout d'abord que, à moins de ne cibler des résidents européens, les praticiens ne sont pas soumis au RGPD, mais uniquement à la loi fédérale en matière de protection des données, dont une révision devrait entrer en vigueur dans le courant de l'année 2022.

2. *Obligations légales*

Sans entrer dans les détails, les praticiens sont de prime abord soumis à trois obligations, dont il convient cependant de relativiser la portée pour les deux premières :

1. Le registre des activités de traitement

L'obligation faite aux praticiens de tenir un registre des activités impose en principe de déterminer, entre autres, le type de traitements, leur raison d'être, les catégories de personnes (patients, employés, parfois fournisseurs) et les catégories de données personnelles (qui peuvent s'avérer sensibles dans le domaine médical) traitées, tout comme les éventuels transferts à l'étranger et destinataires de ces possibles transferts.

Le Conseil fédéral a cependant exempté les entreprises ayant moins de 250 employés de cette obligation lorsque les traitements concernés n'impliquent pas le traitement de données sensibles à grande échelle ou ne conduit pas à l'établissement de profilage à risque élevé. Or, si l'établissement d'un profilage à risque élevé apparaît d'emblée exclu pour les praticiens, le traitement de données sensibles est certes possible, notamment dans le domaine médical. Toutefois, l'exigence de « grande échelle » semble supposer une exploitation massive au sein d'un établissement hospitalier ou d'une clinique ce qui, de prime abord, ne devrait dont pas être le cas d'un cabinet privé.

Voici donc une obligation dont les praticiens devraient être exemptés.

2. L'obligation d'information

Tout responsable de traitement, dont les praticiens font partie, ont en principe l'obligation d'informer la personne concernée de manière adéquate de la collecte de données personnelles qu'elle effectue, et de la raison d'être de cette collecte (concrètement, il faut expliquer ce que l'on va en faire et pourquoi il est nécessaire de les collecter).

Si une telle obligation est facile à mettre en œuvre, la loi prévoit toutefois que lorsque le responsable de traitement est une personne privée soumise à une obligation légale de garder le secret, il est alors délié de cette obligation. Or, les praticiens sont justement soumis à une telle obligation de par l'art. 321 du Code pénal ; partant, il faut en conclure qu'ils n'ont pas d'obligation légale d'informer leurs patients ou clients des traitements opérés.

A ce principe, une exception néanmoins. Lorsque le traitement envisagé exige le traitement de données sensibles, comme des données médicales, le consentement exprès de la personne concernée est alors exigé, ce qui implique alors que cette dernière soit dûment informé du traitement concerné pour que son consentement soit valablement donné, étant précisé qu'en droit suisse, à la différence du droit européen, le consentement est considéré comme exprès même s'il se fait par un renvoi à des conditions générales.

3. Les mesures de sécurité adéquates

Au final, ce sont en réalité les obligations faites aux praticiens de s'assurer que des mesures de sécurité adéquates ont été mises en place pour protéger les données par rapport aux risques encourus qui sont les plus importantes.

A partir de là, quels sont les conseils que l'on peut donner aux praticiens ?

3. *Considérations pratiques*

1. Sur le plan technique

Trois remarques :

- Tout d'abord, le fait que le praticien doit s'assurer que son infrastructure garantit une forme de sécurité aux données de ses patients ou clients. A cet égard, on relèvera qu'il est désormais largement admis que le recours à un **fournisseur cloud** est admissible en tant que ce dernier apparaît comme un auxiliaire (au même titre que le personnel administratif) du praticien ; lui confier le traitement des données n'apparaît donc pas comme une violation de l'art. 321 CP. On veillera tout d'abord dans l'idéal à ce que les serveurs du fournisseur en question soient en Suisse ou, à tout le moins, en Europe (point de vue ici contesté quant à l'admissibilité d'avoir ou non pour les praticiens un fournisseur en dehors de la Suisse, mais en Europe), et qu'ils fassent l'objet de certaines certifications comme gages de sécurité, telle la norme ISO27001. Rien n'interdit évidemment cependant aux praticiens d'avoir un **serveur interne dûment protégé** par un firewall ou un VPN lorsque l'exercice de la profession, notamment pour les avocats et le télétravail, entraîne du travail à distance.

- Ensuite, mettre en place un **contrôle des accès**, puisque rien ne justifie le plus souvent que tout le personnel administratif ait accès à toutes les données, potentiellement sensibles des patients traités, ni même que chaque employé sache combien ses collègues sont payés. Le principe anglo-saxon du « *need to know basis* » devrait ici s'appliquer.

- Enfin, on évitera de recourir à des adresses emails peu professionnelles comme le font hélas certains dans le domaine médical comme hotmail, Gmail ou bluewin, le recours à un système de messagerie instantané comme What's App étant de surcroît à prescrire dans l'univers professionnel, sauf requête et accord exprès (et insistant serais-je tenté d'ajouter) du patient ou client. Le cryptage des emails, aujourd'hui aisé (voir un fournisseur comme www.swisssign.com), est à recommander.

2. Sur le plan informationnel

Quand bien même nous avons vu que l'obligation d'information était en réalité cantonnée aux traitements de données sensibles (comme les données médicales) pour lesquelles un consentement exprès est exigé, il est néanmoins aisé et à mon sens de bon aloi de favoriser ici une certaine transparence, ce qui peut se faire à moindres efforts de deux manières :

- Tout d'abord, en adoptant une **politique en matière de confidentialité** à faire figurer sur son site ou comme flyer dans sa salle d'attente, qui recoupe le plus souvent les points suivants : (1) quelles sont les données traitées ; (2) dans quels buts ?; (3) avec qui partageons-nous vos données ? (4) où sont-elles traitées ?, (5) combien de temps les conservons-nous ? et (6) quels sont vos droits ? Tel a du reste été le choix de Wilhelm Gilliéron Avocats SA qui, spécialisée en matière de protection des données, se voyait difficilement ne pas avoir de politique en la matière, que vous trouverez ici.

- Ensuite, et plus particulièrement dans le domaine médical où il est usuel de devoir remplir un **formulaire** avant toute consultation, le recours audit formulaire est un moyen pratique et facile pour y mentionner la raison d'être de la collecte de certaines données (en particulier de santé et pour lesquelles le consentement exprès est requis), la manière dont elles sont conservées, pour quelle durée et avec qui elles sont partagées.

3. Divers

Enfin, on ne saurait trop attirer l'attention sur le fait que tout transfert de données à l'étranger ne devrait se faire qu'avec l'accord exprès de la personne concernée, et qu'il importe de supprimer après un lapse de temps à déterminer (généralement défini par la loi) les données traitées une fois que la personne concernée n'est plus patiente ou cliente (20 ans par exemple pour les médecins-dentistes).

4. *Conclusion*

Si la loi fédérale en matière de protection des données et le grand buzz médiatique que ce domaine entraîne a de quoi effrayer, il est pourtant aisé pour ceux qui exercent en la forme libérale de s'y conformer en prenant un nombre de mesures sommes toutes minimes : une politique en matière de confidentialité adéquate, un formulaire qui permette de s'assurer du consentement exprès en cas de traitement de données sensibles (même si une signature n'est en soi pas absolument nécessaire) et, surtout, des mesures de sécurité adéquates n'exigeant cependant que la prise de mesures sommes toutes assez simples.

Source : https://www.wg-avocats.ch/actualites/protection-des-donnees/protection-donnees-professions-liberales/