Etudes d'avocats: se mettre en conformité avec la LPD et le RGPD

DR

Anne Dorthe,
avocate.

Suite à l'entrée en vigueur du RGPD, le 25 mai 2018, le cadre légal en matière de protection des données s'est renforcé. Etant donné qu'elles traitent diverses données personnelles (notamment de clients et d'employés), les études d'avocats sont directement concernées.

Une étude suisse doit s'organiser pour être en conformité avec le droit de la protection des données actuellement en vigueur et prendre un certain nombre de mesures. Elle ne saurait renier ses obligations, sous prétexte qu'elle est protégée par le secret professionnel qui couvre les activités traditionnelles d'un avocat.

L'ampleur des mesures à mettre en place nécessite que chaque étude consacre un certain temps et des ressources à sa mise en conformité.

1. Une étude d'avocats suisse est-elle soumise à la LPD?

Oui, elle est soumise à la Loi fédérale sur la protection des données (LPD) ainsi qu'à son Ordonnance (OLPD).

Une étude d'avocats est une personne privée au sens de l'art. 2 LPD, peu importe qu'elle soit organisée sous la forme d'une SA, d'une Sàrl ou d'une société simple.

Son but principal est la fourniture de prestations juridiques par des avocats. Dans ce cadre, elle traite un grand nombre de données à caractère personnel, relatives à des personnes physiques ou morales, telles que l'adresse postale, le numéro de téléphone, l'adresse e-mail, les données financières, les liens familiaux, la santé, le casier judiciaire, les opinions politiques. L'usage de données dans un cadre professionnel est en principe soumis à la LPD[1].

A notre sens, une étude d'avocats ne peut exciper de l'art. 2 al. 2 let. c LPD pour soutenir qu'elle n'est pas soumise à la LPD et à l'OLPD. Effectivement, elle traite également de données personnelles relatives à ses employés, ses prospects, ses prestataires et ses clients hors procédure judiciaire, entre autres. Ces mêmes données ne tombent pas sous le coup de cette exception.

2. Une étude d'avocats établie exclusivement en Suisse est-elle soumise au RGPD?

Elle est susceptible de l'être.

L'art. 3 al. 2 RGPD a un effet extraterritorial, car il prévoit que le RGPD s'applique au traitement de données personnelles d'individus qui se trouvent sur le territoire de l'Union par un responsable de traitement qui n'est pas dans l'Union, si ce dernier offre des biens ou des services à ces personnes dans l'Union.

Ainsi, toute étude proposant des services à une clientèle locale et internationale (site web en anglais, assistance à des personnes physiques ou morales sises dans l'UE voulant s'implanter en Suisse, numéro de téléphone international, etc.), et dont la clientèle est effectivement suisse et européenne, est à notre sens soumise au RGPD, et doit donc s'y conformer.

3. Quels types de données traite une étude d'avocats?

Les données qu'une étude traite peuvent être personnelles, sensibles, ultrasensibles, confidentielles.

Les données personnelles sont toutes celles qui se rapportent à une personne identifiée ou identifiable, étant précisé que le RGPD se limite aux personnes physiques, tandis que la LPD actuelle protège tant les personnes physiques que les personnes morales.

Certaines de ces données peuvent être sensibles. Ce sont, par exemple, celles qui touchent aux opinions ou aux activités religieuses, philosophiques, poli-

tiques ou syndicales, à la santé, à la sphère intime ou à l'appartenance à une race, à des mesures d'aide sociale, à des poursuites ou des sanctions pénales et administratives d'une personne (art. 3 let. c LPD). Contrairement à la LPD, le RGPD distingue les données relatives à la santé, la religion, la vie sexuelle, l'appartenance syndicale, etc. (art. 9 RGPD: «Catégories particulières») de celles sur des condamnations pénales et infractions, dont le traitement est extrêmement limité (art. 10 RGPD).

Les données ultrasensibles sont celles dont la divulgation peut entraîner des risques très élevés, en particulier en lien avec la vie de la personne concernée[2].

Nous sommes d'avis qu'une étude prudente devrait qualifier les données relatives de ses clients d'ultrasensibles et confidentielles.

iStock

4. Quelles sont les mesures nécessaires pour être en conformité avec le RGPD et la LPD?

A titre liminaire, rappelons que tout traitement de données doit respecter, que ce soit en application de la LPD ou du RGPD, les principes de la licéité, de la bonne foi, de la proportionnalité, de la finalité, de la reconnaissabilité, de l'exactitude et de la sécurité des données. L'étude devra ainsi procéder à son examen à la lumière de ces principes.

Selon notre analyse, une étude établie en Suisse soumise à la LPD et au RGPD devrait mettre en place, à tout le moins, les mesures suivantes:

4.1. Désigner une (ou plusieurs) personne en charge de la protection des données

Même si cette mesure n'est pas obligatoire du point de vue légal, chaque étude composée de plusieurs acteurs devrait nommer une (ou plusieurs) personne en charge de la mise en conformité de l'étude et qui travaillerait en étroite collaboration avec le service informatique (interne ou externe)[3]. Sa fonction consisterait principalement à organiser et à superviser la mise en place effective des mesures idoines. Elle pourrait, le cas échéant, être nommée DPO si tant est qu'elle remplisse les conditions.

4.2. Documenter sa conformité dans un dossier

Dans ce dossier, l'étude décrira les mesures mises en place et les décisions prises, subsidiairement les étapes tendant à sa conformité, afin de disposer des éléments de preuve en cas de contrôle. Cette documentation répond au principe d'*accountability*, grande nouveauté du RGPD qui consacre le principe de responsabilité active du responsable de traitement.

[1] Philippe Meier, Protection des données, Fondements, principes généraux et droit privé, Stämpfli, Berne, 2011, p. 187.

[2] Guide relatif aux mesures techniques et organisationnelles de la protection des données, publié par le PFPDT en août 2015, p. 4/30.

[3] A. Amiguet et P. Fischer, Changement de paradigme en matière de protection des données, Revue de l'avocat, 1/2018, pp. 28 ss, p. 34.

L'étude réunira notamment les PV de son conseil, le registre des activités de traitement, la politique de confidentialité, ses procédures internes en lien avec la protection des données, les contrats avec les sous-traitants, etc.

4.3. Tenir un registre des activités de traitement

L'étude tiendra un tel registre, ce même lorsqu'elle compte moins de 250 employés, puisque les données traitées de manière non occasionnelle peuvent être sensibles, voire ultrasensibles.

Ce registre répertoriera les informations relatives aux caractéristiques des traitements mis en œuvre par l'étude listées à l'art. 30 RGPD. Il permettra d'avoir en tout temps une vue d'ensemble des données traitées.

La LPD actuelle n'exige pas qu'une étude tienne un tel registre, mais celui-ci présente une utilité manifeste, notamment pour cartographier les traitements effectués et déterminer s'il y a une communication transfrontière impliquant des mesures supplémentaires.

4.4. Adopter une procédure interne de traitement des demandes

Afin de s'assurer que les demandes seront traitées adéquatement, l'étude adoptera une procédure interne expliquant aux collaborateurs à qui transmettre une telle demande, comment (par e-mail, oralement, autre), quelles conditions doivent être remplies pour donner suite positivement, dans quel délai la demande doit être traitée, etc.

L'étude s'efforcera de donner suite (négativement ou positivement) dans un délai de 30 jours à la requête de la personne concernée (clients, employés, prestataires, etc.) tendant à l'effacement, la modification, la rectification, l'accès ou l'obtention d'une copie de ses données (art. 1 OLPD, 12 al. 3 RGPD et art.12 al. 3 et 17 ss RGPD).

Afin de centraliser les demandes, il est conseillé de créer une adresse e-mail dévolue (par exemple «dataprotection@etude.ch») et de la rediriger vers l'adresse e-mail personnelle du ou des collaborateurs en charge de la protection des données (ou du DPO). Il suffirait de mentionner cette adresse sur le site internet de l'étude (par exemple dans la politique de protection des données) et/ou dans le contrat qui sera conclu.

4.5. Obtenir le cas échéant le consentement de certaines personnes

A l'issue de l'établissement du registre des activités de traitement, l'étude devra réfléchir si et à qui elle doit demander un consentement préalable. Il s'agit par exemple des personnes faisant usage du formulaire de contact sur le site internet, des destinataires de la newsletter de l'étude.

Dans ce cadre, afin d'éviter de devoir insérer un «bandeau de cookies» peu attrayant sur son site internet, nous recommandons de faire usage d'un outil de statistiques ne collectant pas les adresses IP des visiteurs, tel que Matomo. A défaut, il faudra obtenir le consentement des utilisateurs pour être conforme au RGPD.

4.6. Informer au sujet des traitements de données à caractère personnel

Le devoir d'information doit être distingué du devoir d'obtenir le consentement.

En fonction des traitements effectués, l'étude peut avoir l'obligation de communiquer des informations. Dans certains cas seulement, elle pourra se prévaloir du secret professionnel pour refuser, restreindre ou différer l'information.

Il y a pléthore de moyens de communication, tels que la politique de confidentialité disponible sur le site internet, le règlement du personnel, une clause contractuelle, une note d'honoraires, etc. C'est davantage les informations communiquées que la forme du message qui importent.

Le RGPD prévoit une longue liste d'informations à fournir, variant en fonction de la personne auprès de laquelle les données sont collectées (art. 14 RGPD). Si la récolte a lieu auprès de tiers, l'avocat pourra être dispensé de fournir la moindre information (art. 14 al. 5 RGPD).

4.7. Former les collaborateurs à la protection et à la sécurité des données

Certes, aucune disposition légale ne traite expressément de cette formation du personnel. Cela étant, cette mesure organisationnelle est, à notre sens, implicitement exigée par les lois actuellement en vigueur.

4.8. Sélectionner des sous-traitants et conclure un contrat protégeant les données

Pour ses activités, l'étude collabore avec de multiples sous-traitants (par exemple, hébergement de son site internet, maintenance du parc informatique, etc.). Elle doit sélectionner ceux présentant des garanties suffisantes pour assurer la mise en œuvre des mesures de sécurité et de confidentialité appropriées et conclure avec eux un contrat répondant aux exigences de l'art. 28 RGPD.

Tout au long de la relation contractuelle, l'étude devra s'assurer régulièrement que les garanties sont respectées.

4.9. Sécuriser les données personnelles

Selon l'art. 7 al. 1 LPD, les données personnelles doivent être

protégées contre tout traitement non autorisé par des mesures organisationnelles et techniques appropriées, ce en vue d'assurer la confidentialité, l'intégrité et la disponibilité des données. L'art. 9 OLPD précise cette disposition en énumérant une liste non exhaustive («notamment») d'objectifs. Ces mesures doivent également garantir que, par défaut, seules les données nécessaires au regard de chaque finalité sont traitées (*Privacy by default*, art. 25 al. 2 RGPD). L'étude s'efforcera de mettre en place ces mesures dès le début de ses activités (*Privacy by design*, art. 25 al. 1 RGPD).

Comme le relève la doctrine, «il est simplement inconcevable que l'avocat se contente de les conserver [les données informatiques] sur son ordinateur personnel ou le serveur installé dans les locaux de son étude. Il ne satisferait pas à son devoir de diligence, puisqu'il serait à la merci des effets d'une panne ou d'un incendie et exposé au risque de ne pouvoir ni accomplir son mandat correctement ni rendre compte de son travail, comme il le doit aux termes de l'art. 400 CO.»[4]

En d'autres termes, pour respecter l'art. 400 CO et l'art. 12 let. a LLCA, l'étude doit mettre en place un certain nombre de mesures techniques et organisationnelles aux fins de protéger les données de ses clients, en tenant compte du risque élevé à très élevé.

Le Préposé fédéral a publié sur son site internet un guide intitulé «Guide relatif aux mesures techniques et organisationnelles de la protection des données»[5], qui permet de faire un état de la situation.

On peut citer les exemples suivants:

– Sécuriser les locaux de l'étude (y compris salles de serveurs et d'archives) et contrôler les accès, par exemple en attribuant des badges personnels limitant les accès, en plaçant des alarmes, en journalisant les accès, en confiant le nettoyage des locaux à une personne connue qui ne déléguera pas sa tâche, en adoptant une procédure d'accueil pour les visiteurs, etc.

– Sécuriser les places de travail en mettant à disposition des rangements qui peuvent être fermés à clé, en installant les antivirus idoines, en installant les places de travail de telle sorte que les écrans d'ordinateurs ne soient pas visibles depuis la porte ou la fenêtre, etc.

– Identifier et authentifier chaque utilisateur avec un identifiant et un mot de passe attribué à chaque collaborateur. Le Préposé fédéral suggère même d'exiger de l'utilisateur, une fois qu'il est connecté à sa machine de travail, qu'il s'identifie encore une fois pour accéder au logiciel qui contient les données de clients (par exemple Winlex). En ce qui concerne les mots de passe, il conseille qu'ils soient forts (avec huit caractères, dont des lettres majuscules et minuscules, des caractères spéciaux et des chiffres) et changés régulièrement.

– Sécuriser l'accès aux données et aux serveurs de l'étude. Il convient d'adopter une organisation interne qui définisse les droits d'accès de chaque collaborateur en appliquant le principe du moindre privilège *(Privacy by default)* (par exemple la personne en charge de la comptabilité n'a pas besoin d'avoir accès aux documents du dossier, uniquement les time-sheets et coordonnées du client) et de la mettre en place concrètement.

– En cas de cloud computing, l'étude prendra des mesures supplémentaires, à savoir disposer d'une connexion internet de qualité et suffisamment rapide et un câblage suffisant, installer un système de switch efficace, privilégier un data center en Suisse et offrant un système de sécurité accrue.

– Sécuriser l'accès à distance au serveur de l'étude, notamment en mettant en place une méthode d'authentification forte et en limitant les accès aux e-mails sur les téléphones portables, eu égard au risque accru de perte ou de vol.

– Sécuriser l'intégration des données de clients et journaliser les traitements et les accès. Chaque collaborateur susceptible d'introduire des données sera formé à cette activité. L'étude utilisera des données fictives ou anonymisées pour les tests et journalisera tous les traitements effectués sur les données, notamment leur introduction, leur modification, leur accès, leur transfert (expéditeurs et destinataires, trajet effectué, points intéressants du trajet), leur destruction et conservera les «fichiers logs» de journalisation pour une durée d'une année (art. 10 al. 2 OLPD). S'agissant de la journalisation, l'étude informera les collaborateurs qu'une trace des actions qu'ils effectuent sur les données est conservée et elle sécurisera les logs issus de la journalisation.

– Chiffrer les données du fichier clients à l'aide d'une clé de chiffrement longue, au vu de la sensibilité des données. Cette clé sera sécurisée et son accès sera limité à un nombre restreint de collaborateurs.

– Sécuriser les supports (par exemple clé USB) sur lesquels des données sont enregistrées ainsi que leur transmission. L'étude remettra aux collaborateurs des supports externes chiffrés et exigera qu'ils ne fassent usage que de ceux-ci.

– Définir une procédure de sauvegarde des données, afin d'assurer leur intégrité et leur disponibilité et la communiquer aux collaborateurs.

– Procéder à la récupération des données uniquement par du personnel formé à cette tâche, à savoir le service IT.

[4] B. Chappuis, A. Alberini, Secret professionnel de l'avocat et solutions cloud, Revue de l'avocat 2017, p. 340.

[5] www.edoeb.admin.ch > protection des données > documentation > guides.

– Adopter une politique d'archivage et de conservation, qui pourra, par exemple, prévoir que le dossier clients est archivé, dès le terme du mandat, sur la base d'un numéro et non d'un nom. Il faudrait prévoir une table de correspondance des dossiers archivés avec le numéro attribué au dossier. La date d'archivage devra être tenue et son accès limité grâce au chiffrement. Il serait également judicieux de conserver les dossiers archivés dans une base spécifique distincte de la base active, afin notamment de devenir inaccessibles aux personnes n'ayant plus d'intérêt à les traiter. L'étude pourra adresser, dix ans après la date d'archivage, un courrier à la personne concernée (client, employé, etc.), afin de savoir si elle souhaite que son dossier (sous format papier et électronique, y compris CD et autres supports) soit détruit, conservé par l'étude ou restitué.

– Effacer les données électroniques, si la personne concernée en donne l'instruction, à l'aide de programmes spéciaux qui garantissent un effacement physique et définitif des données, procéder à la destruction du dossier sous format papier par une déchiqueteuse et à la destruction des supports mobiles.

– Intégrer la signature et le chiffrement asymétrique des messages.

4.10. Adopter une procédure interne en cas de violation de données personnelles

Cette procédure a pour but d'expliquer à tout collaborateur quel comportement adopter lorsqu'il a connaissance d'une violation de données personnelles (à qui l'annoncer, sous quelle forme, dans quel délai, etc.).

4.11. Notifier toute violation de données personnelles

Aux termes de l'art. 34 RGPD, l'étude a l'obligation de notifier à l'autorité de contrôle toute violation de données personnelles dans les meilleurs délais et, si possible dans un délai de 72 heures au plus tard après en avoir pris connaissance, et éventuellement à la personne concernée s'il y a un risque élevé (art. 34 RGPD). Les art. 33 al. 3 et 34 al. 3 RGPD énumèrent les éléments que les notifications doivent contenir.

Contrairement au RGPD, la LPD actuelle n'impose pas à une étude suisse de notifier au Préposé une violation de données personnelles.

5. Quelles sont les mesures non obligatoires?

Sans distinction de taille, les études d'avocats ne sont pas soumises à l'obligation de déclarer leurs fichiers au Préposé fédéral.

Dans sa publication intitulée «Exceptions à la déclaration»[6], le Préposé s'en explique: «Conformément à la loi fédérale sur la libre circulation des avocats, ces derniers sont tenus d'exercer leur profession avec soin et diligence. La tenue de dossiers corrects, complets et cohérents concernant chaque cas fait partie intégrante de cette obligation; en ce sens, ce traitement de données repose sur une obligation légale.»

Sous l'angle du RGPD, un avocat qui exerce à titre individuel peut se prévaloir du § 91 RGPD et arguer qu'il ne fait pas de traitement à grande échelle, pour renoncer aux mesures suivantes:

a. Procéder à une analyse d'impact
b. Nommer un DPO
c. Nommer un représentant dans l'Union

La question de savoir si les études d'avocats, même de taille réduite, peuvent également se prévaloir du § 91 RGPD demeure en suspens. Une étude prudente devrait envisager de mettre en place ces trois mesures, qui plus est si sa taille est importante.

6. Conclusion

L'entrée en force du RGPD le 28 mai 2018 et la refonte actuelle de la LPD ont mis la protection des données sur le devant de la scène. Ce sujet nécessite la plus grande attention des études d'avocats suisses, quand bien même elles n'auraient pas d'établissement dans l'Union européenne. En effet, le RGPD est exigeant et formaliste et diverses mesures doivent être mises en place, nonobstant le secret professionnel de l'avocat. Elles doivent procéder à un examen minutieux en fonction de leurs propres activités et de leur taille.

[6] https://www.edoeb.admin.ch/edoeb/fr/home/protection-des-donnees/handel-und-wirtschaft/entreprises/declaration-des-fichiers.html