UTILISATION DES SERVICES DE CLOUD PAR LES AVOCATS

CHRISTIAN SCHWARZENEGGER
Prof., Dr, avocat, Université de Zurich

FLORENT THOUVENIN
Prof., Dr, avocat, Université de Zurich

BURKHARD STILLER
Prof., Dr, Université de Zurich

DAMIAN GEORGE
avocat, MLaw, Université de Zurich

Mots-clés: services de *cloud,* secret professionnel, droit de la protection des données

L'utilisation des services de *cloud* par les avocats soulève des questions de droit pénal et de protection des données, qui font parfois l'objet de controverses en doctrine. Le présent article démontre qu'en principe, ces services peuvent en l'état être utilisés par les avocats. Ce texte constitue une version abrégée d'un rapport préparé par ses auteurs pour la Fédération suisse des avocats en automne 2018. Le rapport complet sera publié dans la collection du Center for Information Technology, Society, and Law (ITSL) de l'Université de Zurich.

I. Introduction

Depuis longtemps, l'utilisation de services informatiques est indispensable à l'exercice de la profession d'avocat. Souvent, la mise en place et la maintenance du système informatique ne sont pas assurées par l'avocat lui-même, mais par des informaticiens internes ou un prestataire de services informatiques externe. Depuis peu, les cabinets d'avocats utilisent non seulement des ordinateurs autonomes ou des réseaux locaux, mais également des services de *cloud.* Le terme *«cloud»* décrit des services en ligne accessibles, via un réseau, depuis n'importe quel endroit, de sorte que leur emplacement physique peut être négligé d'un point de vue technique.

Cette évolution soulève la question de savoir si et à quelles conditions les avocats travaillant en Suisse peuvent utiliser les services de *cloud* pour le traitement, le stockage et l'archivage de documents et autres fichiers dans le cadre de leur activité professionnelle. Pour répondre à cette question, il convient d'examiner si l'utilisation de services de *cloud* constitue une violation du secret professionnel au sens de l'article 321 CP (III) et si elle est compatible avec les dispositions de la loi sur la protection des données (IV). Il convient en outre de clarifier au préalable les fondements techniques (II).

II. Fondements techniques

1. Les modèles de services de cloud

Presque toutes les ressources informatiques peuvent être externalisées sur un *cloud* et il existe différents modèles de services de *cloud* sur le marché. On en distingue généralement trois grandes catégories: *Infrastructure-as-a-Service* (IaaS), *Platform-as-a-Service* (PaaS) et *Software-as-a-Service* (SaaS). Le modèle de service PaaS est principalement utilisé pour le développement d'applications. Dès lors que les cabinets d'avocats n'utilisent que rarement ce modèle de service à l'heure actuelle, la description qui suit se limitera aux deux autres modèles.

A) Infrastructure en tant que service (IaaS)

L'*Infrastructure-as-a-Service* (IaaS) est le modèle de base des services de *cloud.* Avec ce modèle, les ressources de *cloud* (par exemple, l'informatique, le stockage ou l'accès au réseau) sont mises à disposition en tant que service. Ce modèle est une option intéressante si une étude d'avocats a besoin d'une infrastructure assistée par ordinateur, mais ne souhaite pas l'exploiter lui-même pour des raisons financières. Avec ce modèle, l'étude d'avocats continue de déterminer quelles solutions logicielles seront installées et doit également prendre des mesures pour assurer la

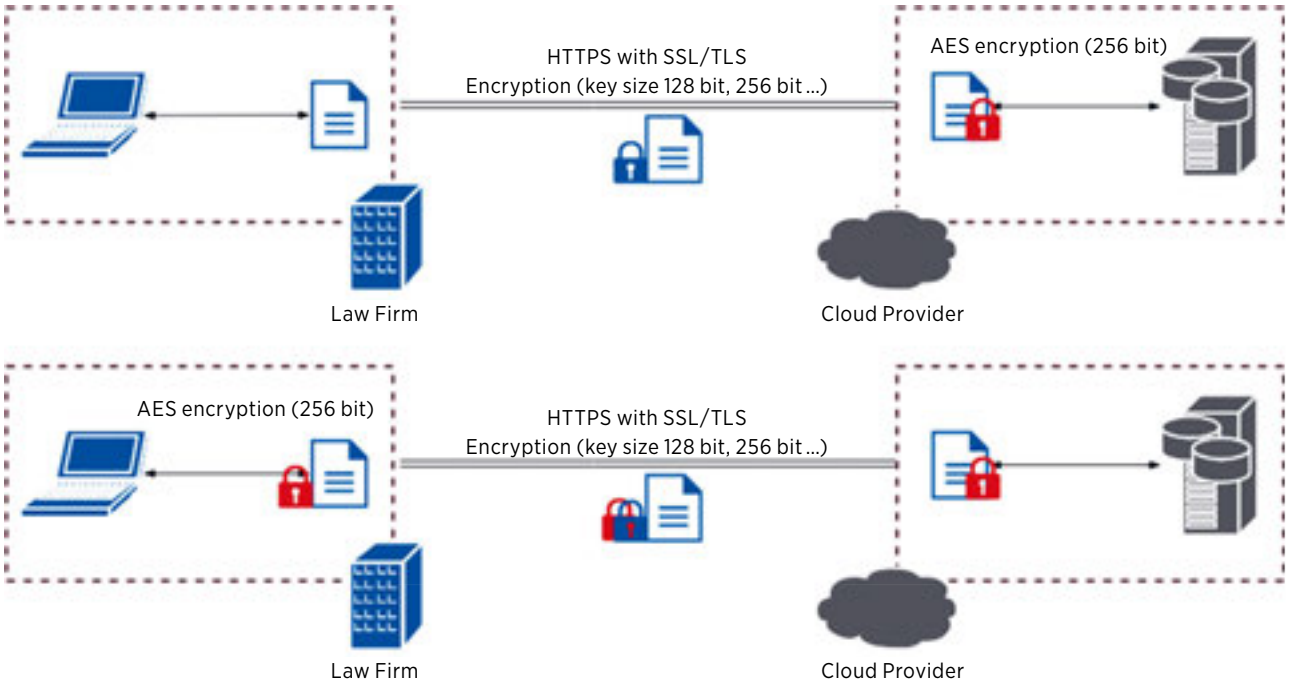

Illustration 1: Cryptage et gestion des clés dans le modèle de service IaaS

confidentialité et l'intégrité du système. Le fournisseur de *cloud* doit, quant à lui, s'assurer que les données stockées par l'étude d'avocats sont disponibles à tout moment.

B) Software-as-a-Service (SaaS)

Avec le *Software-as-a-Service* (SaaS), le fournisseur de *cloud* fournit sur Internet une application logicielle conviviale pour l'utilisateur final. Avec ce modèle de service, ce ne sont pas seulement les logiciels et les données qui sont stockés de manière centralisée sur le *cloud,* mais également le traitement des données (par exemple traitement de texte, calcul ou création de présentations). Le fournisseur de *cloud* installe également des mises à jour et offre des fonctions de support. Contrairement à l'IaaS, le modèle de service SaaS permet à l'étude d'avocats de ne réaliser que des configurations limitées en matière de sécurité. D'un point de vue technique, il lui suffit d'assurer la sécurité des données d'accès. Il appartient au fournisseur de services de *cloud* d'assurer la confidentialité des données, l'intégrité du réseau et la disponibilité des services.

2. L'accès aux données

Lors de l'utilisation des services de *cloud,* les données ne sont plus stockées localement dans l'étude d'avocats, mais chez le fournisseur de services de *cloud.* La transmission sur Internet est cryptée par HTTPS (Hypertext Transmission Protocol Secure) et TLS (Transport Layer Security)[1], lesquels utilisent une clé de grande taille (128 ou 256 bits). Le fournisseur de *cloud* chiffre également les données à l'aide d'une clé locale, par exemple la méthode de cryptage AES (Advanced Encryption Standard).

Le modèle de service Iaas peut se présenter de deux manières différentes: si les données sont cryptées par le fournisseur de *cloud,* tant l'étude d'avocats que le fournisseur de *cloud* ont accès aux données (voir la partie supérieure de l'illustration 1). Les données à stocker par le fournisseur de *cloud* peuvent également être cryptées par l'étude d'avocats, avant d'être transmises sur Internet (voir la partie inférieure de l'illustration 1). Ainsi, seul l'étude d'avocats a accès aux données.

Dans le modèle de service SaaS (illustration 2), le fournisseur de services *cloud* rend le logiciel disponible dans le *cloud.* L'application logicielle doit pouvoir accéder aux fichiers non cryptés et les données sont donc lisibles par le fournisseur de services *cloud.* Les autres utilisateurs du même *cloud* ne peuvent toutefois pas accéder à ces données, car une clé différente est utilisée pour chaque client. Cela étant, les clients qui travaillent avec des contenus confidentiels doivent être conscients, lorsqu'ils utilisent le SaaS, que le fournisseur de *cloud* peut accéder à leurs données et qu'il a la possibilité de les utiliser.

III. Condamnation pénale: violation du secret professionnel

Selon l'art. 321 du Code pénal suisse, les détenteurs du secret professionnel et leurs auxiliaires (III. 2) sont punissables, sur plainte, s'ils révèlent un secret qui leur a été confié (III. 1) à un tiers non autorisé (III. 3) et agissent intentionnellement et sans motif justificatif.

1 TLS est la version mise à jour de SSL (Secure Socket Layer) 3.0 qui a été classée obsolète par l'Internet Engineering Task Force (IETF) dans le document RFC 7568.

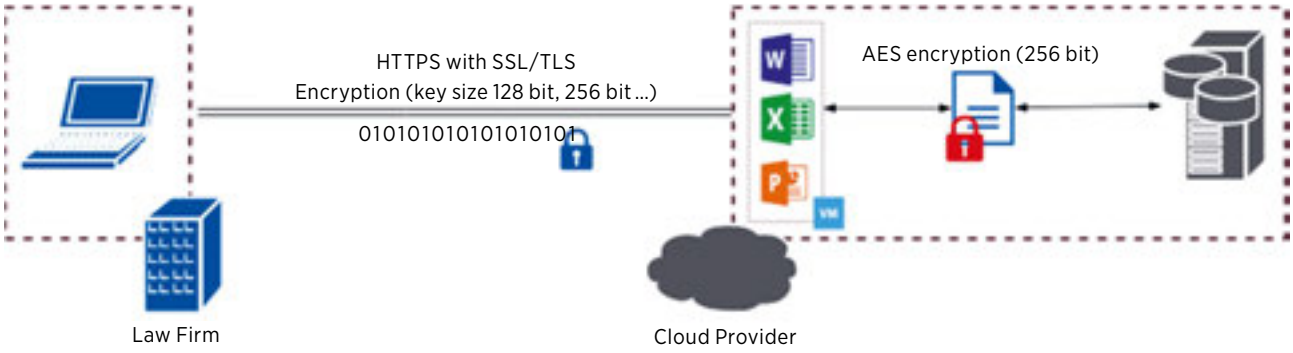

Illustration 2: Cryptage et gestion des clés dans le modèle de service SaaS

1. L'objet de l'atteinte: le secret protégé

Les secrets au sens matériel sont juridiquement protégés. Un secret doit porter sur un fait non connu de chacun. Cela est le cas lorsqu'un nombre restreint de personnes possèdent l'information en question. Un secret existe si le maître du secret a un intérêt légitime et la volonté de garder l'information confidentielle[2]. L'art. 321 du Code pénal suisse (CP) couvre l'ensemble des informations confiées à l'avocat dans l'exercice de sa profession et obtenues dans ce cadre-là. Il n'est pas nécessaire que l'information fasse référence au client, ni qu'elle ait été délibérément communiquée ou transmise à l'avocat[3]. Les informations provenant d'activités commerciales juridiques dites accessoires, comme la gestion de fortune, les opérations de dépôt, le recouvrement de créances et les mandats au sein de conseils d'administration[4] ou les informations acquises dans le cadre de la vie privée de l'avocat ne sont pas couvertes par le secret professionnel au sens de l'art. 321 ch. 1 al. 1 CP.

2. Les auteurs: les personnes détentrices du secret et les auxiliaires

A) Les détenteurs du secret

L'art. 321 CP est un véritable délit spécial, ce qui signifie que seuls les professionnels explicitement et exhaustivement énumérés dans la disposition peuvent en être les auteurs[5]. Les avocats sont nommément cités, de même que les défenseurs en justice[6], les notaires et les conseils en brevets et autres groupes professionnels[7]. La catégorie des avocats comprend toutes les personnes qui ont suivi une formation professionnelle appropriée et sont titulaires d'un certificat de compétence suisse ou étranger, qui pratiquent ou non dans le cadre du monopole[8]. L'inscription au registre des avocats n'est pas déterminante[9].

B) Les personnes auxiliaires

Les auxiliaires au sens de l'art. 321 ch. 1 al. 1 CP sont tenus au secret au même titre que le détenteur (principal) du secret. L'interprétation de la notion d'auxiliaire d'un membre de la profession tenu au secret professionnel est déterminante. Sa signification peut être précisée en se fondant sur les méthodes d'interprétation usuelles.

Selon l'interprétation grammaticale, les auxiliaires sont des personnes qui assistent quelqu'un dans l'accomplissement d'une tâche. Le sens littéral couvre tous les types d'assistance, qu'il s'agisse de travaux de dactylographie, de recherche, de courses ou d'assistance à la gestion des données. Même les prestataires de services infor-

2 Cf. ATF 127 IV 122, c. 1; 142 IV 65, c. 5.1 d. et les références citées (ad art. 320 CP); NIGGLI, Gutachten betreffend Anwendung von Art. 321 StGB auf angestellte Unternehmensjuristen (In-house lawyers), Fribourg 2005, www.swissholdings.ch/fileadmin/kundendaten/Dokumente/Archiv_Publikationen-Publikation/05-08-05-Gutachten_Niggli.pdf, page consultée pour la dernière fois le 19. 12. 2018, p. 20 ss et les références citées; OBERHOLZER, in: Basler Kommentar Strafrecht II, 3e éd., Bâle 2013, CP 321 N 14; STRATENWERTH/BOMMER, Schweizerisches Strafrecht, Besonderer Teil II: Straftaten gegen Gemeininteressen, 7e éd., Berne 2013, § 61 N 5; TRECHSEL/VEST, in: Schweizerisches Strafgesetzbuch, Praxiskommentar, 3e éd., Zurich 2018, CP 321 N 20 ss et les références citées.

3 Ainsi déjà GAUTIER, Procès-verbal de la deuxième Commission d'experts concernant le Code pénal, Lucerne 1915, tome 4, p. 365; NIGGLI, Unterstehen dem Berufsgeheimnis nach Art. 321 StGB auch Unternehmensjuristen? Eine Verteidigung des materiellen Strafrechts gegen die Freunde des Verfassungsrechts, zugleich eine Antwort auf Pfeifer, Revue des Avocats 2006, p. 279; OBERHOLZER (nbp 2), CP 321 N 16; TRECHSEL/VEST (nbp 2), CP 321 N 21 s.

4 Cpr ATF 143 IV 462, c. 2.2; NIGGLI (nbp 2), p. 21 ss; TRECHSEL/VEST (nbp 2), CP 321 N 21. La protection pénale ne vise que l'activité typique des avocats, même si, dans la pratique, il est parfois difficile de la distinguer de l'activité atypique (cf. arrêt du TF 1B_85/2016 du 20. 9. 2016, c. 6 sur la délégation de tâches de compliance au sens de la LBA à une étude d'avocats).

5 ZÜRCHER, Schweizerisches Strafgesetzbuch, Erläuterungen zum Vorentwurf vom April 1908, Berne 1914, p. 351; OBERHOLZER (nbp 2), CP 321 N 11; TRECHSEL/VEST (nbp 2), CP 321 N 3; STRATENWERTH/BOMMER (nbp 2), § 61 N 17; WOHLERS, Auslagerung einer Datenbearbeitung und Berufsgeheimnis (Art. 321 StGB), Rechtsgutachten im Auftrag des Datenschutzbeauftragten des Kantons Zürich, Zurich 2016, p. 13.

6 Selon le Code de procédure pénale, la défense des personnes accusées d'un crime ou d'un délit est réservée aux avocats qui, selon la LLCA, sont habilités à représenter les parties devant les autorités judiciaires (art. 2 LLCA, art. 127 al. 5 CPP). La mention supplémentaire de défenseurs en justice n'a donc qu'une propre signification dans les procédures pénales pour infraction.

7 Pour en savoir plus sur les différents groupes professionnels OBERHOLZER (nbp 2), CP 321 N 5 ss; TRECHSEL/VEST (nbp 2), CP 321 N 6 ss.

8 NIGGLI (nbp 2), p. 15, p. 19 s.

9 OBERHOLZER (nbp 2), CP 321 N 6.

matiques qui assurent le traitement des données pour la personne détentrice du secret peuvent être assimilés à des auxiliaires.

On remarque, d'un point de vue systématique, que les auxiliaires visés à l'art. 321 ch. 1 al. 1 CP sont mentionnés de la même façon que les (principaux) détenteurs du secret et sont soumis à la même menace de sanction. Cela laisse penser que le législateur a voulu élargir le cercle des personnes qui auraient connaissance de faits confidentiels, en se basant sur une conception fonctionnelle de l'environnement de travail.

L'interprétation historique apporte également des indications claires. Il ressort des travaux préparatoires qu'une conception restrictive de la notion d'auxiliaire a été explicitement rejetée. Les doutes émis par deux membres de la commission d'experts, qui recommandaient de limiter l'interprétation du terme «auxiliaire», ont été entendus mais n'ont volontairement pas été pris en compte[10]. De même, dans la consultation parlementaire, la référence au fait que l'expression «Gehilfen solcher Personen» était quelque peu vague n'a donné lieu à aucune discussion, ni même à une adaptation de la disposition pénale[11].

D'un point de vue téléologique également, cela n'a aucun sens de limiter de manière étroite le cercle des auxiliaires. Si on retenait une définition restrictive du terme, le détenteur du secret devrait traiter personnellement tous les documents confidentiels, maintenir lui-même les systèmes d'exploitation informatiques et gérer lui-même les données afin d'exclure la possibilité d'accès par des tiers non autorisés tels que le personnel de nettoyage, les secrétaires ou le personnel informatique. Cependant, la loi ne peut être comprise comme exigeant des processus pratiquement impossibles à mettre en œuvre sur le plan opérationnel, ou du moins très inefficaces[12].

La protection suisse du secret professionnel repose donc sur une compréhension large et fonctionnelle de la personne auxiliaire[13]. Une personne auxiliaire au sens de l'art. 321 CP est toute personne qui participe à l'activité professionnelle d'un détenteur (principal) du secret de manière à lui permettre en principe d'en prendre connaissance.

3. L'acte délictueux: la révélation du secret

A) La prise de connaissance

L'élément constitutif objectif de la révélation est rempli si la personne à qui le secret a été confié le porte à la connaissance d'un tiers qui n'y est pas autorisé ou permet à ce tiers d'en prendre connaissance. Selon la jurisprudence du Tribunal fédéral et la doctrine majoritaire, la prise de connaissance par un tiers est requise pour la réalisation de l'infraction[14]. Toutefois, l'acte peut également être commis par omission[15], par exemple par une conservation inadéquate des dossiers[16].

Dans le cas d'informations anonymisées ou cryptées, il n'y a pas de révélation car il est impossible d'en prendre connaissance[17]. L'archivage de données cryptées dans un *cloud* (modèle de service IaaS) ne remplit pas les éléments constitutifs objectifs de l'art. 321 CP (voir II. 1. A). Avec le

10 ALFRED GAUTIER a ainsi souligné les problèmes de délimitation dans la deuxième commission d'experts: «Car il est délicat de délimiter le cercle de ces auxiliaires. On risque d'y comprendre de simples petits comparses sur lesquels ne doit reposer aucune responsabilité spéciale, …» (GAUTIER [nbp 3], p. 365). La commission d'experts n'a pas développé cet argument. Conformément à GAUTIER, EUGÈNE DESCHENAUX a déposé une motion demandant que le terme «auxiliaire» soit remplacé par «assistant ou employé supérieur» afin d'exonérer les employés subordonnés de toute responsabilité pénale éventuelle (procès-verbal de la deuxième Commission d'experts sur le Code pénal, Lucerne 1915, tome 4, p. 371). La proposition DESCHENAUX a été rejetée par la commission d'experts à une large majorité (*ibid.,* p. 376).

11 Bulletin sténographique du Conseil national, 26. 9. 1929, p. 612.

12 Exiger le consentement du détenteur du secret pour toutes ces activités ne peut représenter une solution pour les mêmes raisons. Par exemple, avant tout changement organisationnel, comme le recrutement de stagiaires et de personnel de secrétariat ou la nomination d'une société de nettoyage, il faudrait obtenir les déclarations de consentement de tous les clients. Cela semble inapproprié, puisque le travail est en partie délégué et que la personne à qui sont confiés les secrets serait rapidement confrontée à un nombre trop important de demandes de consentement.

13 WOHLERS interprète cela de manière étroite, en se basant sur le § 203 de l'ancien Code pénal allemand. Il s'appuie en particulier sur une figure juridique jusqu'alors inhabituelle dans la doctrine suisse, à savoir le «Kreis der zum Wissen Berufenen». Cette notion implique que le maître du secret désigne une personne ou un groupe de personnes avec qui il souhaite partager le secret (WOHLERS [nbp 5], p. 16, 18 et 26; WOHLERS, Outsourcing by Professional Secrets, digma 2017, p. 116). Ce concept n'est toutefois pas compatible avec la jurisprudence et la doctrine suisses: arrêt du 18. 11. 2015 du Tribunal d'arrondissement de Zurich, GG 150233, c. II.2.5.2, «Der Kreis der Hilfspersonen ist praktisch unbegrenzt»; CHAPPUIS/ALBERINI, Secrets professionnel de l'avocat et solutions Cloud, Revue de l'Avocat 2017, p. 339 ss; KELLER, Das ärztliche Berufsgeheimnis gemäß Art. 321 StGB unter besonderer Berücksichtigung der Regelung im Kanton Zurich 1993, p. 106 ss et les références citées avec une restriction au «professionnel»; NIGGLI (nbp 2), p. 30 s.; OBERHOLZER (nbp 2), CP 321 N 10; TRECHSEL/VEST (nbp 2), CP 321 N 13; STRATENWERTH/BOMMER (nbp 2), § 61 N 17, avec une limitation au «professionnel». Cf. NATER/ZINDEL in: Kommentar zum Anwaltsgesetz: Bundesgesetz über die Freizügigkeit der Anwältinnen und Anwälte (Anwaltsgesetz, BGFA) BGFA, 2e éd., 2011, Zurich, LLCA 13 N 51 s. et N 53: «Massgeblich ist vielmehr sowohl strafrechtlich als auch berufsrechtlich, ob die Tätigkeit der Hilfsperson die Möglichkeit des Zugangs zu geschützten Informationen einschliesst».

14 Arrêt du TF 6B_1403/2017 du 8. 8. 2017, c. 1.2.2; ISENRING, StGB/JStG-Kommentar, Orell Füssli Kommentar, 20e éd., Zurich 2018, CP 321 N 10b; DONATSCH/THOMMEN/WOHLERS, Strafrecht IV: Delikte gegen die Allgemeinheit, Zürcher Grundrisse des Strafrechts, 5e éd., Zurich 2017, p. 580 s.; OBERHOLZER (nbp 2), CP 320 N 10.

15 OBERHOLZER (nbp 2), CP 321 N 19; STRATENWERTH/BOMMER (nbp 2), § 61 N 7 und 19; STRAUB, Aufbewahrung und Archivierung in der Anwaltskanzlei, AJP 2010, p. 552 und 555; TRECHSEL/VEST (nbp 2), CP 321 N 23. Toutefois, si l'on présume qu'un tiers non autorisé a pris connaissance de l'information confidentielle, l'infraction ne peut être réalisée par un stockage inadéquat de l'information en question, qui constituerait tout au plus une tentative punissable.

16 En ce qui concerne les exigences relatives à l'archivage des fichiers, les dispositions de l'art. 7 LPD et de l'art. 8 OLPD peuvent être appliquées, étant donné qu'il s'agit de fichiers au sens de la LPD, qui contiennent souvent des données particulièrement sensibles au sens de l'art. 3 lit. c LPD. Les avocats sont dispensés de l'obligation de déclaration prévue à l'art. 11*a* LPD, cf. BLECHTA, in: Basler Kommentar Datenschutzgesetz/Öffentlichkeitsgesetz, 3e éd., Basel 2014, LPD 11a N 14d. S'agissant du stockage: BLECHTA *(ibid.),* LPD 7 N 7 ss.

17 BERGER, Outsourcing vs. Geheimnisschutz im Bankgeschäft, recht 2000, p. 191 et les références citées; BLATTMANN, in: Praxiskommentar zum Informations- und Datenschutzgesetz des Kantons Zürich, Zurich 2012, Gesetz über die Information und den Datenschutz (IDG) 6 N 13; TRECHSEL/VEST (nbp 2), CP 321 N 23; WOHLERS (nbp 5), p. 20; Préposé fédéral à la protection des données et à la transparence, 14e rapport d'activité 2006/2007 pour la période du 1. 4. 2006 au 31. 3. 2007, p. 51.

modèle de service SaaS en revanche, le fournisseur du service de *cloud* a un accès technique aux données stockées (voir II. 2). Dans cette situation, une prise de connaissance des informations confidentielles est dès lors possible.

B) Pas de révélation à des auxiliaires

Le législateur est parti du principe que le responsable du secret avait un environnement professionnel de travail partagé avec d'autres personnes. La coopération entre le détenteur du secret et les auxiliaires implique en effet que ces derniers entrent en contact avec les informations protégées par le secret. Ainsi, les auxiliaires ne peuvent en aucun cas être considérés comme des tiers non autorisés. Ils assistent directement le maître du secret dans sa sphère professionnelle[18], sous sa responsabilité, où règne une confiance mutuelle[19]. Les auxiliaires sont punissables de la même sanction que le (principal) détenteur du secret. Une révélation des secrets à des auxiliaires ou une prise de connaissances ne remplit par conséquent pas le critère objectif de la révélation à des tiers non autorisés[20].

C) Tiers non autorisés

Les tiers non autorisés sont toutes les personnes qui ne sont ni des auxiliaires ni des personnes autorisées à prendre connaissance du secret de par la loi ou en raison d'un consentement. Le détenteur du secret peut également violer son secret professionnel en divulguant les informations confidentielles à d'autres personnes tenues au secret, par exemple en en faisant état à des avocats d'une autre étude[21].

4. Conséquences pour l'utilisation de services de cloud

A) Les fournisseurs de cloud *en tant qu'auxiliaires*

Il résulte de ce qui précède que les fournisseurs de services de cloud doivent être qualifiés d'auxiliaires de l'avocat au sens de l'art. 321 ch. 1 al. 1 CP. Les informations protégées par le secret professionnel peuvent leur être communiquées sans que cela constitue une révélation indue[22].

B) Obligation de diligence dans la sélection, l'instruction et la surveillance

Lors du choix d'un auxiliaire, les personnes astreintes au secret professionnel doivent respecter certaines règles, lesquelles découlent également du droit civil et des règles professionnelles[23]. Celles-ci ne permettent aucune révélation proscrite par le droit pénal[24] mais contribuent à appréhender le concept d'auxiliaire de l'art. 321 ch. 1 al. 1 CP, dans le cadre d'une interprétation téléologique.

Les avocats qui font appel à des auxiliaires sont responsables au sens de l'art. 101 du Code des obligations (CO) pour tous les dommages causés par leurs auxiliaires chargés d'exécuter une obligation, à condition qu'ils puissent être hypothétiquement accusés de tels dommages. L'art. 13 al. 2 LLCA prévoit également que les avocats doivent faire en sorte que le secret professionnel soit respecté, en engageant, instruisant et supervisant leurs auxiliaires[25]. S'ils ne prennent pas toutes les mesures raisonnables pour s'assurer que le secret soit gardé, ils enfreignent cette règle professionnelle[26]. Selon la doctrine, les auxiliaires doivent en outre être contractuellement tenus au secret[27] et, selon la taille et l'activité de l'étude d'avocats, un véritable dispositif de sécurité s'impose[28]. Il peut donc s'avérer nécessaire de restreindre le cercle des personnes auxiliaires impliquées dans des informations particulièrement sensibles et de prendre les mesures techniques et organisationnelles appropriées pour protéger ces informations.

Le maître du secret n'est donc pas complètement libre dans ses actions. Le respect des obligations civiles et professionnelles exige plutôt une limitation raisonnable du cercle des personnes qui ont accès aux informations secrètes et une prise de mesures suffisantes pour sécuriser ces informations.

---

18 DONATSCH/THOMMEN/WOHLERS (nbp 14), p. 590; KELLER (nbp 13), p. 107 s. et les références citées.

19 TRECHSEL/VEST (nbp 2), CP 321 N 25. Cf. ég. les règles de droit civil concernant la responsabilité pour les auxiliaires, art. 101 CO: WIEGAND, in: Basler Kommentar OR I, 6e éd., Bâle 2015, CO 101 N 4 s. Ég. dans ce sens le jugement du 18. 11. 2015 du Tribunal d'arrondissement de Zurich, GG 150233, c. II.2.5.3.

20 De manière explicite: Jugement du 18. 11. 2015 du Tribunal d'arrondissement de Zurich, GG 150233, c. II.2.5.3; ég. STRATENWERTH/WOHLERS, Schweizerisches Strafgesetzbuch Handkommentar, 3e éd., Berne 2013, CP 320 N 3, CP 321 N 4. D'un avis contraire, WOHLERS (nbp 5), p. 21 s. et 25 s.: «Tatsächlich kann (…) aus der Existenz der Kategorie der Hilfspersonen als taugliche Täter *nicht* gefolgert werden, dass auch die Weitergabe an sie *für den primären Geheimnisträger* straflos sein soll. Die Kategorisierung als Hilfsperson ändert deshalb für sich gesehen nichts daran, dass die Weitergabe der Daten als Offenbaren eines Geheimnisses einzustufen ist» (accent mis par les auteurs).

21 ATF 114 IV 44, c. 3.b; BERGER (nbp 17), p. 187; DONATSCH/THOMMEN/WOHLERS (nbp 14), p. 593 et les références citées; ISENRING (nbp 14), CP 320 N 15, CP 321 N 10; KELLER (nbp 13), p. 114 s. et les références
citées; PIETH, Strafrecht, Besonderer Teil, 2e éd, Bâle 2018, p. 131; RASELLI, Amts- und Rechtshilfe durch Informationsaustausch zwischen schwerizerischen Straf- und Steuerberhöden, Revue Pénale Suisse 1993, p. 32 s. et les références citées; STRATENWERTH/BOMMER (nbp 2), § 61 N 7.

22 D'un autre avis, WOHLERS (nbp 5), p. 20, qui considère que le sous-traitant n'est pas un auxiliaire. Dès qu'ils peuvent déchiffrer les informations secrètes du détenteur, ce dernier procède à leur divulgation. Il en va de même pour les prestataires de services informatiques qui sont en charge de la maintenance des logiciels.

23 Selon WOHLERS (nbp 5), p. 16, et WOHLERS (nbp 13), p. 115, sur la base d'une interprétation restrictive, le contrôle du cercle des personnes ayant droit à la confidentialité ne peut être confié à l'avocat.

24 NATER/ZINDEL (nbp 13), LLCA 13 N 16; cf. ég.: WEBER, in: Basler Kommentar OR I, 6e éd., Bâle 2015, CO 398 N 11.

25 SCHILLER, Schweizerisches Anwaltsrecht, Zurich 2009, N 540 ss; cf. ég. CHAPPUIS/ALBERINI (nbp 13), p. 341.

26 SCHILLER (nbp 25), N 540; NATER/ZINDEL (nbp 13), LLCA 13 N 56 s.

27 MAURER/GROSS, in: Commentaire romand, Loi sur les avocats, LLCA, Basel 2010, LLCA 13 N 101; SCHILLER (nbp 25), N 541; NATER/ZINDEL (nbp 13), LLCA 13 N 56; cf. ég. Préposé à la protection des données du Canton de Zurich (Datenschutzbeauftragter Kanton Zürich), Rapport d'activité 2017, p. 18.

28 NATER/ZINDEL (nbp 13), LLCA 13 N 56 s. On peut songer, par exemple, à la gestion des clés, qui reste de la responsabilité de l'entreprise dans les modèles de service IaaS (cf. II.2) II.1.A) ou au contrôle d'accès dans les modèles de service IaaS et SaaS, qui reste toujours de la responsabilité de l'entreprise (cf. II.1.B).

C) Participation des fournisseurs étrangers de services de cloud

Si des données sont transférées à l'étranger ou si un fournisseur étranger de services de *cloud* se voit accorder l'accès à des données stockées en Suisse, ces données peuvent être soumises à une protection juridique plus faible ou à un droit d'accès des autorités étrangères (par exemple dans le cas de mesures coercitives dans une procédure pénale). Par exemple, le *Cloud Act*[29] adopté par le Congrès américain en mars 2018 permet aux autorités américaines d'accéder aux données stockées à l'étranger si elles sont en possession, sous la garde ou le contrôle d'un fournisseur américain de services de cloud[30].

La compétence pénale suisse est en principe liée au lieu de commission de l'acte, i. e. soit le lieu d'exécution ou le lieu du résultat (art. 8 al. 1 CP). Si le secret est révélé à l'étranger, il se peut que ni la commission de l'acte ni le résultat n'aient lieu en Suisse. Toutefois, pour admettre qu'il y a eu communication à un auxiliaire, il n'est pas déterminant que celui-ci soit également soumis à l'art. 321 CP[31]. Ce qui est décisif, c'est que l'implication du fournisseur de *cloud* soit autorisée. Cela implique que ce dernier soit contractuellement tenu au secret professionnel et que l'externalisation prévue résiste à une évaluation des risques[32]. Dans cette évaluation, il faut tenir compte de la sensibilité des données, mais aussi du respect attendu des contrats et des lois auxquels est soumis le fournisseur étranger de services de *cloud,* ainsi que de la réelle probabilité d'accès aux données. Cette évaluation des risques peut varier en fonction de l'activité des avocats; il convient d'être particulièrement prudent notamment lorsque l'on conseille des clients étrangers sur des questions fiscales et des clients politiquement exposés.

5. Garanties supplémentaires: le consentement de l'interessé

Même si le recours à des fournisseurs de services de *cloud* par les avocats est généralement autorisé, il semblerait raisonnable, afin de garantir un degré de sécurité supplémentaire, d'obtenir le consentement des clients pour l'utilisation de fournisseurs de *cloud* (ainsi que pour l'engagement d'autres auxiliaires, telles que des substituts et des responsables informatiques) dans le cadre du contrat de mandat. Ce consentement peut être donné de manière informelle. En outre, un consentement implicite pourrait être présumé si les clients ont suffisamment été informés sur l'utilisation des services de *cloud* par leur avocat et si, cela fait, ils ont été d'accord de poursuivre la relation de mandat. S'agissant des mandats terminés, il convient de prévoir un archivage crypté côté utilisateur dans le cadre d'un modèle de service IaaS, lequel exclut d'emblée l'accès par le fournisseur de *cloud* au contenu des données stockées (voir II. 2).

IV. Appréciation des aspects liés à la protection des données: traitement des données

1. Traitement des données personnelles

Le traitement des données personnelles, c'est-à-dire les informations relatives à une personne identifiée ou identifiable, est soumis aux dispositions de la loi fédérale sur la protection des données (LPD) (art. 2 en relation avec l'art. 3 lit. a LPD).

La loi sur la protection des données ne s'applique pas à l'utilisation des services de *cloud* par les avocats si les fournisseurs de services de *cloud* ne traitent pas les données personnelles. C'est le cas lorsque les données ne sont stockées que par le fournisseur de services de cloud (modèle de service IaaS) et que les avocats cryptent les données avant leur transmission au fournisseur afin que ce dernier n'ait pas accès au contenu des données. Ce n'est pas le cas si les avocats traitent les données sur l'infrastructure des fournisseurs de *cloud computing* (modèle de service SaaS), car ces derniers peuvent accéder au contenu des données (voir II. 2).

Selon la doctrine et la jurisprudence, il y a données personnelles lorsque, d'après l'expérience générale de la vie, on doit compter sur le fait que le sous-traitant acceptera de déployer des efforts pour individualiser une personne[33]. Étant donné que cela ne peut être exclu dans le cadre de l'utilisation de fournisseurs de *cloud* selon le modèle de service SaaS, l'utilisation de ces services par des avocats doit être qualifiée de traitement de données personnelles, qui doit avoir lieu conformément aux dispositions de la LPD.

2. Traitement des données

A) Responsabilité du client

Dans la mesure où le traitement des données personnelles par les avocats est autorisé et où les conditions requises pour le traitement des données de commande conformément à l'art. 10*a* LPD sont remplies, les données peuvent également être traitées par le fournisseur de *cloud.* Les avocats demeurent toutefois responsables, en tant que mandants, du respect des exigences de la loi sur la protection des données[34].

B) Transfert par convention

Le traitement des données personnelles est basé sur un accord (contrat de *cloud*) entre les avocats ou l'étude

29 *Clarifying Lawful Overseas Use of Data Act.* Le *Cloud Act* a été rédigé en réaction à l'arrêt Microsoft v. United States, *829 F.3d 197 (2d Cir. 2016),* par lequel la Court of Appeal for the Second Circuit a décidé que le FBI ne pouvait contraindre Microsoft à divulguer des données si elles étaient stockées sur un serveur en Irlande. Cf. ég. 130 Harv. L. Rev. (2016), p. 769 ss.

30 GAUSLING, Offenlegung von Daten auf Basis des CLOUD Act, Multimedia und Recht 2018, p. 579.

31 D'un avis contraire, SCHWANINGER/LATTMANN, Cloud Computing: Ausgewählte rechtliche Probleme in der Wolke, Jusletter du 11. 3. 2013, N 31 s.

32 Voir ci-dessus III. 4. B).

33 Cf. ATF 136 II 508, c. 3.

34 GRAMIGNA, Cloud-Vertrag, in: Schweizerisches Vertragshandbuch: Musterverträge für die Praxis, 3e éd., Bâle 2017, N 30; BAERISWYL, in: Stämpflis Handkommentar Datenschutzgesetz, Berne 2015, LPD 10a N 2; BÜHLER/RAMPINI, in: Basler Kommentar Datenschutzgesetz/Öffentlichkeitsgesetz, 3e éd., Bâle 2014, LPD 10a N 11; SURY/GOGNIAT, Umzug einer Kanzlei in die Cloud, Revue de l'Avocat 2015, p. 204.

d'avocats et le prestataire de services, en l'occurrence le fournisseur de *cloud.*

C) Traitement comme pour le client

Les fournisseurs de services de *cloud* ne peuvent traiter que les données personnelles transmises par les avocats qu'ils seraient eux-mêmes autorisés à traiter (art. 10*a* al. a LPD). Dans la mesure où les exigences de la loi sur la protection des données sont respectées, que le traitement des données personnelles par les avocats est conforme ou repose sur un motif justificatif, les données peuvent être traitées non seulement par les avocats mais aussi par les fournisseurs de services de *cloud.* En revanche, le traitement par les fournisseurs de services de *cloud* pour leurs propres besoins n'est pas autorisé[35]. Afin de s'assurer que le fournisseur de services de *cloud* ne traitera pas les données différemment que les avocats, la manière dont le fournisseur de services de *cloud* traitera les données devrait être décrite dans le contrat ou dans une annexe au contrat[36]. Il peut ainsi être indiqué que les données – sous réserve d'instructions spéciales – ne peuvent être traitées que pour l'exécution du contrat[37].

D) Absence d'obligation de confidentialité contradictoire

Le traitement de données personnelles par des tiers n'est pas autorisé si une obligation légale ou contractuelle de garder le secret l'interdit (art. 10*a* al. 1 let. b LPD)[38]. Comme indiqué ci-dessus[39], l'utilisation des services de *cloud* par les avocats ne constitue pas une violation des obligations légales de confidentialité. Il est toutefois concevable que le contrat prévoie une obligation de confidentialité qui s'oppose à une telle externalisation.

E) Obligations de garantie et de surveillance, en particulier de la protection des données

Étant donné que les avocats sont responsables du respect des exigences de la loi sur la protection des données[40], ils sont tenus de sélectionner avec soin, d'instruire et de surveiller le fournisseur de *cloud*[41]. En particulier, ils doivent veiller à ce que le fournisseur de services de *cloud* garantisse la sécurité des données (art. 10*a* al. 2 LPD), c'est-à-dire la confidentialité, la disponibilité et l'intégrité des données (art. 8 al. 1 OLPD). Pour cette évaluation, il est possible de faire appel à un spécialiste indépendant afin de vérifier les mesures de sécurité du fournisseur de *cloud*[42]. Il est également possible de s'appuyer sur un système de gestion de qualité certifié par le fournisseur de *cloud* selon ISO 9001 ou ISO 27001 ou sur une certification spécifique à la protection des données (par exemple GoodPriv@cy, VDSZ:2014 ou ePrivacy).

3. Externalisation à l'étranger

Si des personnes de l'étranger peuvent accéder aux données stockées dans un *cloud* (en particulier lors de l'utilisation d'un fournisseur de cloud à l'étranger et dans le cadre de la télémaintenance), il y a communication transfrontalière des données (art. 6 LPD)[43]. S'il existe une législation adéquate en matière de protection des données dans le pays en question, cela ne pose généralement pas de problème au regard de la loi sur la protection des données (art. 6 al. 1 LPD). Conformément à l'art. 7 OLPD, le Préposé fédéral à la protection des données et à la transparence publie une liste des États assurant un niveau de protection adéquat[44]. Pour les États qui ne figurent pas sur cette liste, comme les États-Unis d'Amérique, les avocats doivent obtenir des garanties suffisantes en matière de protection des données. Ces garanties peuvent être de nature contractuelle ou découler de l'autocertification du fournisseur d'accès dans le cadre du Swiss-US Privacy Shield[45].

4. Excursus: Règlement européen sur la protection des données (RGPD)

Le règlement européen sur la protection des données (RGPD) peut s'appliquer aux activités des avocats suisses, en particulier si ceux-ci orientent (également) leurs activités vers des clients européens (art. 3 al. 2 RGPD)[46]. Toutefois, l'applicabilité du RGPD peut également résulter de la LDIP, puisque la partie lésée peut, en cas d'atteinte à sa personnalité, choisir le droit de l'État où il a sa résidence habituelle ou le droit de l'État dans lequel le résultat de

35 BAERISWYL (nbp 34), LPD 10a N 26.
36 ROSENTHAL, in: Handkommentar zum Datenschutzgesetz sowie weiteren, ausgewählten Bestimmungen, Zurich 2008, LPD 10a N 71.
37 ROSENTHAL (nbp 36), LPD 10a N 72.
38 BAERISWYL (nbp 34), LPD 10a N 29; du même avis: WOHLERS (nbp 13), p. 115.
39 Cf. ci-dessus, III. 4.
40 Cf. ci-dessus, IV. 2. A).
41 Cf. FF 1988 II 413, p. 463 s.
42 SURY/GOGNIAT (nbp 34), p. 203.
43 ATF 144 I 126, c. 8.3.6; ROSENTHAL (nbp 36), LPD 6 N 7; BÜHLER/RAMPINI (nbp 34), LPD 10a N 22d; GRAMIGNA, Datenschutz und Outsourcing, in: Datenschutzrecht: Beraten in Privatwirtschaft und öffentlicher Verwaltung, Bâle 2015, ch. 20.24; STRAUB, Cloud Verträge – Regelungsbedarf und Vorgehensweise, AJP 2014, 914; SCHWANINGER/LATTMANN (nbp 31), N 15.
44 Cf. <www.edoeb.admin.ch/dam/edoeb/fr/dokumente/2017/04/staatenliste.pdf.download.pdf/liste_des_etats.pdf.>, page consultée pour la dernière fois le 7. 11. 2018; Jugement du 3. 3. 2015 de la Cour d'appel du canton de Zurich, LF140075, c. 3.2; PASSADELIS, Rechtsanwendung bei internationalen Datenbearbeitungen durch Private, in: Datenschutzrecht – Beraten in Privatwirtschaft und öffentlicher Verwaltung, Bâle 2015, ch. 6.44.
45 Cf. Préposé fédéral à la protection des données et à la transparence, Contrat-type pour l'externalisation (outsourcing) du traitement de données à l'étranger, <www.edoeb.admin.ch/edoeb/fr/home/protection-des-donnees/handel-und-wirtschaft/entreprises/declaration-des-fichiers/contrat-type-pour-l-externalisation--outsourcing--du-traitement-.html > ainsi que la liste des entreprises certifiées Swiss-US Privacy Shield du US Department of Commerce, <www.privacyshield.gov/list>, pages consultées pour la dernière fois le 7. 11. 2018.
46 En détail, ZERDICK, in: Beck'sche Kurz-Kommentare, Datenschutz-Grundverordnung, 2e éd., Munich 2018, RGPD 3 N 19; cf. RGPD, consid. 23 ainsi que les arrêts C-585/08 et C-144/09 du 7. 12. 2010 de la Cour de justice des Communautés européennes, Pammer/Alpenhof sur l'interprétation de la notion d'orientation d'une activité. Cf. en outre PRAZ, Responsabilités et outils de conformité selon la RGPD: Obligations du responsable de traitement et du sous-traitant, AJP 2018, p. 610; VASELLA, Zum Anwendungsbereich der DSGVO, digma 2017, p. 220 ss.

l'atteinte s'est produit, pour autant que l'auteur du dommage ait dû s'attendre à ce que le résultat se produise dans cet État. Le RGDP pourrait s'appliquer au traitement de données à caractère personnel dans un *cloud* d'une manière qui porte atteinte à la vie privée, en particulier comme droit du lieu de résidence du client, d'autant que la production du résultat au lieu habituel de résidence du client est généralement prévisible[47].

La situation juridique de l'externalisation du traitement des données au sens de l'art. 28 RGPD correspond en substance à celle de la LPD. L'externalisation dans le cadre du traitement des données est privilégiée et ne doit pas faire l'objet d'une autorisation indépendante au sens de l'art. 6 RGPD[48]. Toutefois, l'art. 28 RGPD, contrairement à la LPD, énonce de manière très détaillée comment le mandant doit se conformer à ses obligations en matière de traitement des données[49]. Le responsable du traitement des données est également un destinataire au sens de l'art. 4 ch. 9 RGPD si des données lui sont communiquées. Le responsable doit communiquer le nom des destinataires des données aux personnes concernées (art. 13 al. 1 let. e RGPD; art. 14 al. 1 let. e RGPD), par une mise à disposition de l'information, par exemple dans une déclaration de confidentialité accessible sur Internet[50].

V. Conclusion

Si les données sont cryptées par des avocats avant d'être transférées à un fournisseur de services de *cloud* et que ce dernier ne dispose pas de la clé, il n'y a pas de révélation de secret au sens de l'article 321 CP. Étant donné que les données cryptées ne peuvent être qualifiées de données personnelles, les activités du fournisseur de *cloud* ne sont pas soumises à la loi sur la protection des données. Dans cette situation, l'utilisation des services de *cloud* par les avocats est dès lors licite, tant du point de vue du droit pénal que du droit de la protection des données.

Si les données sont cryptées par le fournisseur de *cloud* plutôt que par l'avocat, le fournisseur de *cloud* a accès au contenu des données et aux informations protégées par le secret professionnel. Avec l'utilisation de ses services, le fournisseur de *cloud* intègre l'unité fonctionnelle que constitue l'étude d'avocats, dont l'organisation se base sur la répartition des tâches, et doit par conséquent être qualifié d'auxiliaire des avocats en question. Les auxiliaires ne sont jamais des tiers non autorisés au sens de l'art. 321 CP. La révélation d'informations secrètes à des fournisseurs de services de *cloud* ne remplit donc pas le critère objectif de la divulgation à des tiers non autorisés, de sorte qu'il ne peut y avoir de responsabilité pénale en vertu de l'article 321 CP. Toutefois, les avocats doivent choisir avec soin le fournisseur de services de *cloud,* protéger contractuellement le secret professionnel et s'assurer que les données sont utilisées par le fournisseur de services de *cloud* uniquement pour exécuter le contrat. Le respect de ces obligations doit être raisonnablement contrôlé. Du point de vue de la législation sur la protection des données, le recours à des fournisseurs de services de *cloud* en tant que responsables du traitement des données pour les avocats ne pose pas de problème, dès lors que le secret professionnel n'empêche pas le traitement de ces données. Si les autres conditions requises pour le traitement des données sont également remplies, le fournisseur de *cloud* peut traiter les données de la même manière que les avocats sont autorisés à le faire eux-mêmes.

47 ROSENTHAL (nbp 36), LDIP 139 N 26; BÜHLMANN/REINLE, Extraterritoriale Wirkung der DSGVO, digma 2017, p. 10. Le RGPD et le droit national d'application du règlement s'appliqueraient.

48 PLATH, in: DSGVO/BDSG-Kommentar, 3e éd., Cologne 2018, RGPD 28 N 6; SCHMIDT/FREUND, Perspektiven der Auftragsdatenverarbeitung – Wegfall der Privilegierung mit der DS-GVO?, Zeitschrift für Datenschutz 2017, p. 16.

49 L'art. 28 RGPD pourrait dès lors également aider à orienter les responsables de traitement des données suisses.

50 LAUE/NINK/KREMER, Das neue Datenschutzrecht in der betrieblichen Praxis, Baden-Baden 2016, § 3 N 17; cf. ég. KAMLAH, in: DSGVO/BDSG-Kommentar, 3e éd., Cologne 2018, RGPD 12 N 4.