SAV_KANTONE entscheid-der-aufsichtsbeh-C3-B6rde-des-kantons-bern-aa-12-27-vom-17-august-2012

SAV Kantonale Aufsichtsentscheide, FR

Quelle: https://mcp.opencaselaw.ch/entscheid/sav_kantone_entscheid-der-aufsichtsbeh-C3-B6rde-des-kantons-bern-aa-12-27-vom-17-august-2012

Erwägungen

E. 1

Critères de sélection à appliquer par l'avocat·e 3

E. 2

Éléments à intégrer dans le contrat de services informatiques 5

E. 3

La doctrine dominante1 et la jurisprudence2 retiennent que le recours à des fournisseurs de services cloud ne se heurte pas à une contradiction fondamentale avec le secret professionnel de l'avocat·e. De son côté, la Fédération suisse des avocat·es (FSA) constate que la sous-traitance informatique et les services cloud sont devenus la norme dans tous les secteurs de l'industrie et des services. Pour les études d'avocat·es, ces services apportent eux aussi des avantages incontestables. En voici quelques-uns : ■ Par une informatique gérée professionnellement, renforcement de la sécurité des composants matériels et des données exploitées ; ■ Économie au niveau du personnel et du matériel informatique ; ■ Développement continu des fonctionnalités et fiabilité de l'infrastructure informatique ; ■ Accès simplifié à l'infrastructure informatique.

E. 4

La sous-traitance informatique et les services cloud s'accompagnent inévitablement d'une perte de contrôle des données et des systèmes, exposant l'avocat·e à de nouveaux risques, dont les principaux sont les suivants : ■ Risques liés au respect des obligations professionnelles, en particulier celle du secret professionnel de l'avocat·e ; ■ Risques liés à la conformité avec le droit de la protection des données ; ■ Risques contractuels et structurels liés à l'externalisation de services (contrôle des données et de leur stockage, recours à d'autres sous-traitants par le fournisseur cocontractant, vérification de la sécurité des données, garantie de l'accès aux données, etc.).

E. 5

À l'appui de ces explications, l'étude d'avocat·es se doit d'examiner en profondeur les conditions et les limites de la sous-traitance informatique et des services cloud. Parmi les questions fondamentales qui se posent, comment l'avocat·e peut-elle·il concilier son flux de tâches numériques avec ses règles professionnelles (en particulier le secret professionnel de l'avocat·e) et d'autres dispositions (comme celles de la protection des données) ?

E. 6

En publiant les présentes recommandations révisées (sous la forme d'un guide de bonnes pratiques), la FSA souhaite définir, en adéquation des risques et autres aspects techniques, un certain nombre de comportements standard à adopter par l'avocat·e en cas de sous-traitance informatique et de services cloud. Il ne s'agit donc pas de citer la

jurisprudence et de se référer aux discussions doctrinales, mais de présenter, en vue d'une application pratique, les conclusions auxquelles est arrivée la FSA. Tout en privilégiant le 1 YANIV BENHAMOU / FRÉDÉRIC ERARD / DANIEL E. KRAUS, L'avocat a-t-il aussi le droit d'être dans les nuages? Revue de l'avocat, 2019, vol. 22, n° 3, p. 119-12; BENOÎT CHAPPUIS / ADRIEN ALBERINI, Secret professionnel de l'avocat et solutions cloud, Revue de l'avocat 8/2017, p. 337, 338; CHRISTIAN SCHWARZENEGGER / FLORENT THOUVENIN / BURKHARD STILLER / DAMIAN GEORGE, Nutzung von Cloud-Diensten durch Anwältinnen und Anwälte, Revue de l'avocat 1/2019, p. 28 s.; cf. également DAVID ROSENTHAL, Mit Berufsgeheimnissen in die Cloud: So geht es trotz US CLOUD Act, in: Jusletter du 10 août 2020. 2 Cf. arrêt 2C 1083/2017 du 4 juin 2019. 2 | 8

pragmatisme, il convient également de contribuer à la sécurité juridique et de permettre aux avocat·es de continuer à fournir – en vertu du droit auquel elles·ils sont soumis·es – des services compétitifs, fiables et de haute qualité dans le contexte de la transformation numérique.

E. 7

Ces recommandations ont dès lors pour vocation de faciliter l'obtention et l'utilisation de services cloud par les membres de la FSA et s'inscrivent comme un outil permettant d'appréhender en toute lucidité les points à examiner. Elles présentent le cadre juridique et font l'exégèse de certaines normes afin de dissiper les insécurités juridiques ou l'absence de jurisprudence face aux nouveaux défis posés par les services cloud. En marge de ces conseils généraux, il est toutefois cardinal que les études d'avocat·es procèdent à une évaluation appropriée de leurs propres risques et besoins particuliers. II. Terminologie ■ Sous-traitance informatique : externalisation de services par laquelle l'avocat·e confie à un fournisseur externe les activités et les structures informatiques de son étude. ■ Services cloud : mise à disposition d'une infrastructure informatique (espace de stockage, ressources informatiques, applications, etc.), sous la forme de services qui passent par des interfaces techniques et des protocoles internet. L'infrastructure informatique ne réside donc plus matériellement sur des serveurs locaux, mais est fournie à distance par un prestataire de services cloud qui opère en ligne. De nombreuses offres très variées sont proposées, mais l'emplacement physique des données et les mesures de protection comme le chiffrement sont généralement des éléments décisifs. ■ Fournisseurs de services informatiques : auxiliaires de l'avocat·e qui fournissent des services cloud ou accomplissent d'autres services informatiques externalisés. III. Recommandations générales

E. 8

L'avocat·e doit s'assurer que l'infrastructure informatique de son étude et l'intervention de fournisseurs de services cloud restent en conformité avec les exigences réglementaires et légales applicables. Pour l'avocat·e, il s'agit notamment d'exercer sa profession avec soin et diligence3, de ne pas violer son secret professionnel4 et de respecter d'autres impératifs tels que ceux découlant du droit de la protection des données. L'obligation de soin et de diligence constitue le fil conducteur pour le choix de l'infrastructure informatique, de même que pour la sélection, l'instruction et le contrôle du fournisseur de services informatiques. A. Recours à un fournisseur de services informatiques 1. Critères de sélection à appliquer par l'avocat·e

E. 9

Le fournisseur de services informatiques occupera une position de première importance dans l'organisation de l'étude d'avocat·es. Avant de jeter son dévolu sur tel ou tel fournisseur, il conviendra de clarifier en détail plusieurs questions centrales, en particulier 3 Art. 12 let. a LLCA. 4 Art. 13 LLCA et 321 CP. 3 | 8

celle de savoir s'il sera en mesure d'accomplir les tâches confiées avec tout le sérieux et le professionnalisme qu'on peut attendre de lui. Les critères suivants sont décisifs : ■ Son aptitude à exécuter ses obligations contractuelles ; ■ Son expérience et sa réputation ; ■ Son siège et le lieu où il exerce ses activités ; ■ Ses client·es de référence sur le marché des avocat·es ou d'autres prestataires de services : le nombre d'études d'avocat·es ou d'autres détenteurs d'un secret professionnel à qui il offre ses services, leur taille, dans quels pays, etc. ; ■ Sa situation économique (pérennité financière, solvabilité, fiabilité, détention de propriétés et adéquation des fonds propres) ; ■ Nombre de collaborateur·ices déployé·es pour le support et le développement ; ■ Recours à ses propres fournisseurs tiers (sous-traitant de 2ème degré) et degré de dépendance envers eux; ■ Transparence dans les renseignements qu'il fournit à ses client·es : le fournisseur informera-t-il l'avocat·e des réquisitions de données par des autorités nationales ou étrangères, des attaques sur ses serveurs ou dans ses centres de données, etc. ? ; ■ Développement futur des solutions proposées ; ■ Localisation précise de ses serveurs de stockage (surtout s'ils sont à l'étranger) ; ■ Sécurité matérielle et électronique des serveurs et du centre de données ; ■ Si les données sont hébergées à l'étranger (p.ex. parce que le fournisseur est domicilié à l'étranger) ou si elles sont hébergées en Suisse mais qu'il s'agit d'une société, d'un groupe de sociétés ou d'une autre forme de présence à l'étranger (y compris de toute autre possibilité d'accès aux données depuis l'étranger) : examen de la législation civile et pénale applicable in situ, de même que toutes autres dispositions étrangères, en particulier les obligations de divulguer des données de client·es (p. ex. le CLOUD Act des États-Unis d'Amérique) ; probabilité d'occurrence du risque d'un accès aux informations de client·es détenues par l'avocat·e (en fonction de la nature des données).

E. 10

Eu égard à ce qui précède, la sélection du fournisseur de services informatiques s'opère d'abord à la lumière de ses compétences professionnelles ainsi que de ses ressources financières et humaines. Le choix se cristallise ensuite sur les besoins concrets de l'étude d'avocat·es en matière de sécurité des données et des infrastructures, c.-à-d. sur les risques factuels, juridiques et financiers liés à la conservation des données spécifiques des client·es de l'avocat·e. Le fournisseur de services informatiques doit démontrer que l'infrastructure informatique choisie ainsi que son exploitation garantissent, d'un point de vue technique et organisationnel, le niveau de sécurité, de contrôle, d'intégrité et de disponibilité des données requis par l'étude et ses client·es. Au regard de l'art. 211 LP, les précautions nécessaires doivent être prises face à une insolvabilité du fournisseur de 4 | 8

services informatiques. En cas de faillite, les contrats doivent être conçus de manière que l'accès aux données puisse être maintenu ou transféré à un autre fournisseur, ou qu'une infrastructure dite de basculement (mode de sauvegarde opérationnel) soit mise en place.

E. 11

Si le fournisseur cumule plusieurs fonctions informatiques à l'égard de l'avocat·e, il conviendra d'évaluer le risque d'une trop forte concentration des attributions auprès de ce même cocontractant. 2. Éléments à intégrer dans le contrat de services informatiques

E. 12

L’intervention du fournisseur de services informatiques doit être définie dans un contrat écrit. La FSA recommande l’utilisation de l’un des modèles qu’elle a préparés à l’attention de ses membres5, à tout le moins comme feuille de route durant la phase précontractuelle.

E. 13

Voici les points dont l’avocat·e devra tenir compte dans la relation contractuelle qu’iel nouera avec son fournisseur de services informatiques : ■ Si le fournisseur fait appel à ses propres sous-traitants (sous-traitant de 2ème degré): cette sous-traitance doit elle aussi être limitée contractuellement. Si des sous- traitants sont autorisés, ceux-ci doivent être énumérés nominativement. Ils doivent en outre être liés par les mêmes obligations et garanties du fournisseur de services informatiques et l’avocat·e doit être en droit de leur donner des instructions (directement ou indirectement par l’intermédiaire de son fournisseur). Conformément à la jurisprudence fédérale actuelle6, il est toutefois recommandé de s’assurer que les sous-traitants – s’ils ne se sont pas engagés directement envers l’avocat·e à respecter la confidentialité – n’ont aucun accès aux données soumises au secret professionnel de l’avocat·e. Dans ce contexte, on peut notamment envisager un chiffrement des données ; ■ Localisation du traitement et du stockage des données : le contrat précise le lieu où le fournisseur exécute ses services informatiques, d’où il accède aux données et où celles-ci sont stockées ; ■ Clause de confidentialité : le contrat doit prévoir une clause selon laquelle le fournisseur et les éventuels sous-traitants respecteront le secret professionnel de l’avocat·e. Le fournisseur doit être informé qu’il intervient en qualité d’auxiliaire et qu’il est, partant, soumis au secret professionnel (art. 321 CP et 13 LLCA). Il doit s’engager contractuellement à la plus stricte confidentialité, et faire appliquer ses obligations et autres garanties à l’égard de l’avocat·e par ses éventuels sous-traitants mentionnés dans le contrat. Enfin, le fournisseur de services informatiques doit s’assurer que lui-même ou l’avocat·e sont habilités à donner des instructions aux sous-traitants ; ■ Protection des données : le contrat doit garantir que les exigences en matière de protection des données seront dûment appliquées ; ■ Traitement et remise de données à des tiers : le contrat pose le principe selon lequel l’avocat·e conserve en tout temps la propriété des données et que celles-ci devront lui être restituées sur simple demande. Réglementation détaillée en cas de 5 https://digital.sav-fsa.ch/fr/transition-numerique-de-l-etude-cloud-et-protection-des-donn%C3%A9es 6 Cf. arrêt 2C_1083/2017 du 4 juin 2019 5 | 8

faillite du fournisseur (avec une clause de business continuity), de résiliation du contrat (avec garanties de termination assistance et de migration des données), de la possibilité et des modalités de restitution des données ainsi que des obligations si des tiers exigent la production de données (lawful access) ; ■ Accès aux données : le contrat précise (i) quand, (ii) à partir de quel endroit et (iii) à quelle fin le fournisseur de services informatiques, ses employés (en spécifiant lesquels) et ses éventuels sous-traitants peuvent accéder aux données ; ■ Sécurité des données : le contrat définit le niveau de protection et de sécurité des données durant leur transfert, traitement et stockage. Réglementation des obligations d’information du fournisseur de services informatiques si des failles de sécurité ont été constatées ou utilisées abusivement par des tiers ; ■ Service Level Agreement (SLA): le contrat indique en toute clarté les services à fournir, leur disponibilité et leur niveau de qualité. Les attributions de l’avocat·e et du fournisseur doivent être définies et limitées contractuellement, notamment pour les parts de responsabilité découlant d’activités

communes ; ■ Sauvegardes, récupération des données et imprévus : le contrat doit prévoir un mécanisme de sécurité garantissant un rétablissement à brève échéance de toutes les fonctions externalisées, en particulier un accès rapide aux données dans les cas d'urgence (sauvegarde des données, accès à la sauvegarde, connexions de remplacement) ; ■ Droits de donner des instructions et de procéder à des contrôles : ces droits doivent être définis contractuellement entre l'avocat·e et le fournisseur de services informatiques (et directement ou indirectement ses sous-traitants). L'avocat·e peut soumettre les services et l'infrastructure du fournisseur informatique (et directement ou indirectement ses sous-traitants) à un audit de sécurité des données et d'exécution des obligations contractuelles (préservation de la confidentialité, respect de la protection des données, etc.) ; ■ Durée contractuelle : en cas de résiliation par le fournisseur, l'avocat·e doit disposer d'un délai raisonnable pour trouver des solutions de remplacement ; ■ Concours du fournisseur lors de la résiliation du contrat : le contrat énumère les obligations du fournisseur pour accompagner l'avocat·e et faciliter la recherche d'un autre fournisseur de services (maintien de la conformité aux normes, assistance durant le transfert de données termination assistance, migration des données, etc.). Le rétablissement de la fonction externalisée doit être garanti. 3. Surveillance à exercer par l'avocat·e

E. 14

Le maintien des obligations essentielles du fournisseur (respect du secret professionnel et utilisation des données uniquement à des fins d'exécution contractuelle) doit faire l'objet d'une surveillance en adéquation des risques encourus7.

E. 15

Pour des études d'une taille raisonnable et présentant un profil de risque faible (en fonction de la nature des données), il suffit généralement de faire appel à un expert indépendant pour vérifier le dispositif de sécurité du fournisseur de services cloud. Se référer à son système de gestion de la qualité est également envisageable, pour autant qu'il réponde 7 CHRISTIAN SCHWARZENEGGER / FLORENT THOUVENIN / BURKHARD STILLER / DAMIAN GEORGE, op. cit., p. 32 6 | 8

aux normes ISO 9001, 27 001 ou à une certification spécifique à la protection des données (par exemple GoodPriv@cy, OCPD : 2 014 ou ePrivacy).

E. 16

Quelle que soit la taille de l'étude, les avocat·es effectueront régulièrement une batterie de tests, dont : ■ Est-il possible d'accéder aux sauvegardes et, cas échéant, de rétablir les données ? ■ Les logiciels antivirus sont-ils à jour ?

E. 17

En fonction de la taille et des activités de l'étude d'avocat·es, il peut être judicieux de disposer de son propre système de sécurité. Dans ce cas, la fonction sous-traitée au fournisseur doit être intégrée au système de contrôle ou de sécurité informatique de l'étude d'avocat·es. Ces systèmes doivent être conçus en fonction du profil de risque des données de l'étude d'avocat·es. Ce faisant, l'avocat·e doit systématiquement identifier, surveiller, quantifier et gérer les risques importants liés au fonctionnement de son infrastructure informatique et à sa sous-traitance. Dans le cas d'informations particulièrement sensibles, des mesures techniques et organisationnelles appropriées doivent être prises pour protéger de telles données. Le respect des obligations de droit civil et professionnel nécessite de

restreindre de manière appropriée le groupe de personnes autorisées à accéder aux données de la·du client·e. B. Renseignements à fournir par l'avocat·e à son client 1. Information de la·du client·e sur la présence d'un fournisseur externe

E. 18

Au regard du droit professionnel des avocat·es et de la protection des données en vigueur, l'intervention d'un fournisseur de services informatiques ne requiert pas obligatoirement le consentement préalable de la·du client·e. En revanche, la future LPD introduira une obligation générale d'informer son client.

E. 19

Pour contribuer à la transparence, il est conseillé – dès maintenant – d'informer les client·es de la sous-traitance informatique et de l'emploi de moyens de communication électroniques, que ce soit dans les procurations ou les documents contractuels du mandat. L'avocat·e peut ainsi obtenir le consentement de son client. Cet accord ne requiert aucune forme particulière et peut être donné par actes concluants, par exemple lorsque la·le client·e commence lui-même à recourir à de tels services informatiques ou moyens de communication.

E. 20

Dans la mesure où l'avocat·e utilise, dans l'exécution du mandat, certains services informatiques et moyens de communication électroniques (Skype, courrier électronique, Google Docs, Office 365, traitement de données à l'étranger, etc.), il convient d'en informer la·le client·e dans le contrat de mandat et de le rendre attentif, d'une manière générale, aux risques de sécurité des données. Si la·le client·e commence lui-même à recourir à de tels services ou moyens de communication, l'obligation de l'avocat·e devient caduque. 2. Insertion d'une clause dans le contrat de mandat (proposition de la FSA)

E. 21

La FSA recommande d'inclure la clause suivante (ou une disposition comparable) dans le contrat de mandat entre l'étude d'avocat·es et la·le client·e : 7 | 8

Nous attirons votre attention sur le fait que, dans le cadre de nos services, nous faisons appel à des fournisseurs de services informatiques externes et à des fournisseurs de cloud avec des serveurs en Suisse [ou à l'étranger]8 et que nous utilisons certains services informatiques ainsi que des moyens de communication qui peuvent être liés à des risques en matière de sécurité des données (courrier électronique, Skype, Google Docs, DropBox, etc.) Si vous souhaitez que vos données fassent l'objet de mesures de sécurité particulières, il vous appartient de nous en informer. Décision du Conseil FSA du 11 novembre 2022. 8 Le contrat de mandat devra en outre intégrer les dispositions nécessaires en matière de protection des données. 8 | 8