EUROPEAN LAWYERS
EUROPEAN BARS
CCBE
BARREAUX EUROPÉENS
AVOCATS EUROPÉENS

Conseil des barreaux européens
La voix des avocats européens

Rue Joseph II, 40/8 - B-1000 Bruxelles
+32 (0)2 234 65 10 | ccbe@ccbe.eu | www.ccbe.eu

Lignes directrices du CCBE sur l'usage de l'informatique en nuage par les barreaux et les avocats

27/02/2025

Table des matières

I. Introduction

1. Champ d'application des lignes directrices

Ces lignes directrices visent à mieux faire connaître les différents risques liés à l'usage de l'informatique en nuage dans la pratique juridique. Une mise à jour de la version précédente, datant de 2012, était nécessaire afin de refléter les changements survenus dans la législation, les évolutions technologiques et la pratique du droit. Les lignes directrices visent également à donner plus de contexte aux barreaux et dans le cadre de leur utilisation des services en nuage. Elles s'adressent aux barreaux membres du CCBE et servent à les aider dans leur rôle de soutien à leurs membres.

2. Contexte

L'usage de l'informatique en nuage et des services reposant sur l'informatique en nuage a augmenté ces dernières années[1]. Dans l'UE, 42,5 % des entreprises de l'UE ont acheté des services d'informatique en nuage en 2023, principalement pour la messagerie électronique, le stockage de fichiers et les logiciels de bureautique. Par rapport à 2021, la part des entreprises achetant des services d'informatique en nuage dans l'UE a augmenté de 4,2 points de pourcentage en 2023[2].

En 2022, le CCBE a mené une enquête sur l'usage de l'informatique en nuage par les avocats[3]. Bien que la plupart des barreaux ne disposent pas d'informations quantitatives sur l'usage de l'informatique en nuage par les cabinets d'avocats, nombre d'entre eux ont indiqué que cette utilisation était en hausse.

Aux États-Unis d'Amérique, les enseignements du rapport de 2023 *Cloud Computing TechReport* de l'American Bar Association (ABA) « *reflètent une forte augmentation de l'utilisation par les avocats de l'informatique en nuage pour la pratique du droit* ». *Selon le rapport de 2022, l'usage de l'informatique en nuage a augmenté de manière notable, passant de 60 % à 70 %. Les avocats exerçant seuls ont ouvert la voie (passant de 52 % à 84 % en un an), suivis par les cabinets d'avocats de petite et moyenne taille (environ 75 %, contre environ 65 %)* »[4].

L'informatique en nuage offre de nombreux avantages, tels que des dispositifs et des sauvegardes plus résistants et la possibilité d'accéder aux données à partir de différents endroits et de différents appareils (téléphones intelligents, ordinateurs portables, ordinateurs de bureau, tablettes, etc.). Elle permet également d'accéder à des prestataires de services qui peuvent n'être disponibles qu'en nuage[5], ainsi qu'à un espace de stockage et à une puissance de traitement

[1] The State of Cloud Computing in Europe and UK, Kinsta, consulté en janvier 2024.
[2] Eurostat, Entreprises achetant des services d'informatique en nuage, UE, 2021 et 2023
[3] Les représentants de 17 délégations ont répondu à l'enquête du CCBE : Autriche (AT), Croatie (HR), Tchéquie (CZ), Danemark (DK), Estonie (EE), France (FR), Allemagne (DE) (réponse du Deutscher Anwaltverein), Grèce (GR), Hongrie (HU), Irlande (IE), Italie (IT), Liechtenstein (LI), Lituanie (LT), Portugal (PT), Espagne (ES), Suède (SE), et Royaume-Uni (UK).
[4] American Bar association (ABA), 2023 Cloud Computing TechReport, janvier 2024
[5] Par exemple, les outils de traduction.

accrus. En outre, l'informatique en nuage peut offrir des solutions de sécurité améliorées et davantage de flexibilité aux utilisateurs. Toutefois, la collecte, le stockage ou le traitement des données dans le nuage, en particulier lorsqu'elles se trouvent à l'étranger, présentent certains risques.

3. Qu'est-ce que l'informatique dématérialisée ?

L'informatique en nuage est un terme général désignant l'infrastructure informatique qui consiste à stocker et à traiter des données et des logiciels à distance dans le centre de données du fournisseur de nuage ou dans des centres de serveurs interconnectés, auxquels on accède en tant que service sur internet. Il convient également de garder à l'esprit que de nos jours, l'informatique en nuage ne concerne pas seulement le stockage de données, mais aussi la prestation de services informatiques qui fonctionnent dans le nuage au lieu d'un serveur local maintenu par l'utilisateur, y compris pour les avocats et le personnel des cabinets d'avocats (par exemple, les services de messagerie pour la communication avec les clients, les outils de visioconférence, etc.).

Selon le *National Institute of Standards and Technology* (NIST) des États-Unis, l'informatique en nuage permet « *un accès réseau omniprésent, pratique et à la demande à un ensemble partagé de ressources informatiques configurables (par exemple, réseaux, serveurs, stockage, applications et services) qui peuvent être rapidement approvisionnées et libérées avec un minimum d'effort de gestion ou d'interaction avec le prestataire de services* »[6]. Cette définition est largement suivie internationalement, notamment par l'Organisation internationale de normalisation (ISO)[7] et l'Autorité bancaire européenne (ABE)[8].

Certains des actes juridiques les plus récents de l'UE ne s'appuient toutefois pas sur cette définition. Par exemple, l'article 2, paragraphe 6 de la directive (UE) 2019/790 du Parlement européen et du Conseil du 17 avril 2019 sur le droit d'auteur et les droits voisins dans le marché unique numérique et modifiant les directives 96/9/CE et 2001/29/CE définissant le « fournisseur de services de partage de contenus en ligne » qui s'appuie sur la définition du « service de la société de l'information » au sens large, et fait référence aux services en nuage (sans les définir) comme un exemple de ce type de services. De même, les définitions juridiques figurant dans des règlements tels que le règlement sur les services numériques (ou le règlement sur les relations entre les plateformes et les entreprises (règlement (UE) 2019/1150) s'appuient également sur le service de la société de l'information plutôt que sur le terme moins juridique mais plus technique et plus courant d'informatique en nuage.

Compte tenu de ces points, les présentes lignes directrices n'introduiront pas de définition nouvelle ou révisée de l'informatique en nuage. Plutôt que de se concentrer sur un terme spécifique, il est plus important d'aborder les différents risques que l'usage des services en nuage peut présenter pour les avocats et leurs clients.

[6] NIST SP 800-145, The NIST Definition of Cloud Computing, septembre 2011
[7] ISO/IEC 22123-1:2023(en) Information technology — Cloud computing — Part 1: Vocabulary
[8] EBA Recommendations on Cloud Outsourcing and the forthcoming Guidelines on Outsourcing Arrangements (2018)

4. Comment l'informatique dématérialisée est-elle réglementée dans l'UE ?

Il existe un certain nombre de législations et de réglementations qui affectent la façon dont les processus d'affaires peuvent être externalisés vers des fournisseurs de services d'informatique en nuage. Du point de vue des obligations professionnelles des avocats, la principale caractéristique des services reposant sur le nuage est le traitement de données par des tiers, incluant probablement la correspondance entre les avocats et leurs clients et d'autres traitements de données à caractère personnel.

À l'échelle de l'Union européenne, la protection de la confidentialité des communications entre l'avocat et son client est reconnue comme principe général du droit de l'Union européenne par la Cour européenne de justice et a une base juridique dans la Charte des droits fondamentaux de l'Union européenne dans ses articles 7 sur le respect de la vie privée et familiale et 47 sur le droit à un recours effectif et à accéder à un tribunal impartial. Si le droit à la confidentialité des communications avec l'avocat n'est pas garanti, le client risque de ne pas avoir la confiance nécessaire pour divulguer pleinement les informations dont l'avocat a besoin pour fournir des conseils juridiques précis et une représentation adaptée à la situation du client. En d'autres termes, le droit du client à un conseil juridique et à un procès équitable serait gravement compromis.

En Europe, l'article 8 de la Charte européenne des droits fondamentaux consacre la protection des données à caractère personnel et l'article 6 le droit à un procès équitable.

La pièce maîtresse de la législation de l'UE régissant le traitement des données à caractère personnel est le règlement général sur la protection des données (RGPD)[9], ses actes d'exécution dans les États membres et les lignes directrices du Conseil européen de la protection des données (CEPD) en la matière. Celles-ci, cependant, ne concernent pas spécifiquement les avocats et leurs obligations, mais ont une application plus générale.

Le RGPD définit les bases juridiques du traitement des données à caractère personnel, les droits des personnes concernées, les obligations des responsables du traitement et des sous-traitants, les exigences en matière de sécurité de l'information, les évaluations des risques et des impacts et les transferts internationaux de données. La majorité des obligations reposent sur ce que l'on appelle les « responsables du traitement des données ». Les avocats doivent partir du principe qu'ils sont les responsables du traitement des données lorsqu'ils fournissent des services juridiques ou se conforment à leurs propres obligations réglementaires[10].

Il est important de noter que les exigences relatives aux transferts internationaux de données, énoncées au chapitre V du GDPR, sont particulièrement pertinentes pour les services dans le nuage puisque ces derniers peuvent être physiquement basés en dehors de l'UE/EEE et ainsi déclencher de nombreuses obligations pour les organisations qui ont recours à ces services, notamment les avocats et les cabinets d'avocats. En effet, les fournisseurs de services basés dans des juridictions situées en dehors de l'UE/EEE sont soumis à des réglementations

[9] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) : https://eur-lex.europa.eu/eli/reg/2016/679/oj

[10] Comité européen de protection des données, 7 juillet 2021, Lignes directrices 07/2020 concernant les notions de responsable du traitement et de sous-traitant dans le RGPD.

différentes et peuvent, à ce titre, autoriser des comportements qui menaceraient le respect des réglementations nationales ou européennes de la part des avocats et des cabinets d'avocats. Un exemple important est la réglementation qui oblige les services répressifs et les services de renseignement des pays tiers à accéder aux données détenues par les sociétés sous leur juridiction, ce qui peut avoir des effets sur la confidentialité des données détenues par le fournisseur en question.

5. Législations étrangères applicables aux données

Chaque fois que des données sont stockées ou traitées dans une juridiction différente de celle de l'avocat, la question se pose de savoir quelles sont les lois qui s'y appliquent. Cette question est d'autant plus importante lorsque les données sont stockées en dehors de l'UE/EEE et qu'il s'agit de savoir si, conformément à la législation de l'UE, les données bénéficient d'une protection équivalente à celle qui s'applique dans l'UE/EEE. Les avocats qui envisagent de faire appel à des fournisseurs de services d'informatique en nuage aux États-Unis devraient prendre note des décisions Schrems I et Schrems II de la Cour de justice de l'Union européenne (CJUE) concernant les mécanismes de transfert de données entre l'UE et les États-Unis. Dans l'arrêt Schrems II, la Cour a déclaré la décision du bouclier de protection de la vie privée de la Commission européenne nulle et non avenue en raison des programmes de surveillance invasifs des États-Unis, rendant ainsi illégaux les transferts de données à caractère personnel sur le principe de la décision du bouclier de protection de la vie privée. En outre, la Cour a stipulé des exigences plus strictes pour le transfert de données à caractère personnel sur la base de clauses contractuelles types de protection des données (CCT)[11]. La Commission européenne a émis une décision d'adéquation pour les transferts de données à caractère personnel entre l'UE et les États-Unis, à condition que le destinataire des données aux États-Unis adhère au cadre de protection des données à caractère personnel, qui fait suite au bouclier de protection de la vie privée, aujourd'hui disparu. En conséquence, il est recommandé aux avocats qui font appel à des fournisseurs de services aux États-Unis de mettre en place un mécanisme de secours pour le transfert de données par l'intermédiaire de ce que l'on appelle les clauses contractuelles types de protection des données (CCT), un ensemble de clauses contractuelles types qui ont été « préapprouvées » par la Commission européenne en vue de leur adéquation.

6. Contexte juridique et politique plus large

En outre, divers aspects des services en nuage sont réglementés par plusieurs autres législations :

- la directive sur les réseaux et les systèmes d'information (SRI2) (2022)[12] (législation à l'échelle de l'UE sur la cybersécurité) ;

[11] Pour plus de détails sur la décision Schrems II : The CJEU judgment in the Schrems II case, European Parliament Research Service, 2020

[12] Directive (UE) 2022/2555 du 14 décembre 2022 concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, modifiant le règlement (UE) no 910/2014 et la directive (UE) 2018/1972, et abrogeant la directive (UE) 2016/1148 (directive SRI 2), JO L 333 du 27/12/2022, p. 80 : https://eur-lex.europa.eu/eli/dir/2022/2555.

- le règlement sur la libre circulation des données à caractère non personnel (2018)[13] (vise à supprimer les obstacles à la libre circulation des données à caractère non personnel entre les différents pays de l'UE et les systèmes informatiques en Europe) ;
- le règlement cybersécurité (2019)[14] (renforce l'Agence de l'Union européenne pour la cybersécurité (ENISA) et établit un cadre de certification de la cybersécurité pour les produits et les services) ;
- le règlement sur les données (2023)[15] (initiative visant à relever les défis et à exploiter les possibilités offertes par les données dans l'Union européenne) ;
- le règlement sur l'intelligence artificielle (cadre législatif général régissant la fourniture et le déploiement des systèmes d'intelligence artificielle) ;
- le règlement sur la cyberrésilience (un autre cadre législatif axé sur le renforcement de la cybersécurité des produits matériels et logiciels à composantes numériques).

L'UE a également mis en place ou facilité les travaux d'un certain nombre de groupes de travail qui ont défini différents codes de déontologie volontaires ou mécanismes de certification. Il s'agit notamment des lignes directrices sur la normalisation des accords de niveau de service dans le nuage (2014) du *Cloud Select Industry Group* (C-SIG)[16] ou du groupe de travail *Switching Cloud Providers and Porting Data 7* qui a défini des exigences détaillées pour l'exportation et l'importation de données du nuage lorsqu'un utilisateur souhaite passer à un autre fournisseur. Les exemples de certains codes de conduite sont les suivants :

- Code de conduite de SWIPO SaaS pour la portabilité des données propres à l'avocat[17] ;
- Code de conduite cloud de l'UE, cybersécurité et systèmes de certification (liés aux problèmes de négociations qui ne sont pas spécifiques aux avocats, mais communs à toutes les PME)[18].

7. Quels sont les risques liés à l'usage de l'informatique en nuage par les avocats ?

Le principal risque lié à l'usage de services en nuage découle du fait que les données sont traitées par un prestataire tiers qui peut avoir externalisé certaines parties de ce traitement à d'autres tiers, et qui peuvent tous être situés à l'étranger, y compris en dehors de l'UE/EEE. Cela soulève des questions concernant :

[13] Règlement (UE) 2018/1807 du Parlement européen et du Conseil du 14 novembre 2018 établissant un cadre applicable au libre flux des données à caractère non personnel dans l'Union européenne, JO L 303 du 28/11/2018, p. 59-68 : https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX%3A32018R1807

[14] Règlement (UE) 2019/881 du Parlement européen et du Conseil du 17 avril 2019 relatif à l'ENISA (Agence de l'Union européenne pour la cybersécurité) et à la certification de cybersécurité des technologies de l'information et des communications, et abrogeant le règlement (UE) no 526/2013 (règlement sur la cybersécurité), JO L 151 du 7/6/2019, p. 15-69 : https://eur-lex.europa.eu/eli/reg/2019/881/oj

[15] Règlement (UE) 2023/2854 du 13 décembre 2023 concernant des règles harmonisées portant sur l'équité de l'accès aux données et de l'utilisation des données et modifiant le règlement (UE) 2017/2394 et la directive (UE) 2020/1828 (règlement sur les
Données), JO L 2023/2854, 22/12/2023 : https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=OJ:L_202302854&qid=1717084009218

[16] Lignes directrices pour la normalisation des accords de niveau de service dans le nuage : https://digital-strategy.ec.europa.eu/en/news/cloud-service-level-agreement-standardisation-guidelines

[17] https://swipo.eu/saas-sector-group/

[18] https://eucoc.cloud/en/home

- le contrôle de l'avocat ou du cabinet sur ses données ainsi que celles de ses clients, tel que la disponibilité des données et des services fournis et l'accès à ceux-ci, la tenue de registres appropriés des activités conformément aux obligations réglementaires ou la garantie de la continuité de la pratique professionnelle et la possibilité de s'opposer efficacement au traitement ;
- la nature confidentielle et privilégiée des données traitées et la menace potentielle qui pèse sur elles en cas de perte, de vol et de divulgation licite ou illicite, d'autant plus que les activités d'un certain nombre d'avocats présentent un intérêt particulier pour les acteurs malveillants ;
- les moyens de garantir l'exactitude, l'exhaustivité et la qualité des données externalisées auprès d'une multitude de fournisseurs de services informatiques en nuage et stockées au fil du temps et sous différents formats (intégrité).

En effet, parmi les trois principales préoccupations liées à l'usage des services en nuage évoquées par les membres du CCBE dans l'enquête du CCBE en 2022 figurent la protection de la confidentialité, le contrôle des données et la cybersécurité globale.

Ces risques peuvent survenir dans de nombreuses situations et à la suite :

- d'un manque de connaissance des capacités du nuage et des subtilités techniques (par exemple, le stockage de données à distance, les restrictions contractuelles de certaines fonctionnalités telles que la sauvegarde et l'accès aux données, le chiffrement, etc.) ;
- d'un manque de compréhension des modèles de fourniture de services en nuage, y compris les revendeurs à valeur ajoutée et les couches supplémentaires de complexité contractuelle, par exemple la longue chaîne d'approvisionnement et la multitude de partenaires utilisés par les fournisseurs de services en nuage ;
- d'une connaissance insuffisante du fournisseur de services, à savoir le risque financier de perdre les frais de souscription payés à l'avance et la perte potentielle des données traitées par le fournisseur ;
- de protections insuffisantes en matière de cybersécurité du côté de l'utilisateur (c'est-à-dire des avocats) (par exemple, un soin insuffisant dans la conservation des données de connexion à un service d'informatique en nuage par ailleurs sécurisé ou l'utilisation de ce que l'on appelle le *shadow-IT,* soit l'informatique fantôme) ;
- d'une connaissance insuffisante des lois et réglementations qui s'appliquent au traitement des données et à l'accès aux données de la part des services répressifs, en particulier dans les juridictions étrangères, ou au traitement ultérieur des données par les fournisseurs de services en nuage ; ou
- de problèmes techniques et du manque d'adhésion des utilisateurs liés à la fonctionnalité, à la facilité d'utilisation ou aux problèmes d'accessibilité (par exemple, le service ne dispose pas de toutes les fonctionnalités requises ou n'est pas utilisable par les avocats soufrant d'une déficience visuelle) ;
- d'un manque de compréhension des conditions d'utilisation en raison du manque de transparence de la part des fournisseurs (associé à la relative facilité d'utilisation et à la disponibilité des solutions) ;
- de l'absence d'examen approfondi des conditions d'utilisation et de la documentation contractuelle associée.

II. Lignes directrices du CCBE sur l'usage des services d'informatique en nuage par les avocats

Les barreaux nationaux, en conseillant ceux de leurs membres qui envisagent de déployer l'informatique en nuage au sein de leur cabinet, devraient chercher à attirer leur attention, entre autres, sur les considérations suivantes.

1. Obligations professionnelles

L'usage de services d'informatique en nuage engage plusieurs principes fondamentaux de la profession d'avocat, tels qu'énoncés dans la *Charte des principes essentiels de l'avocat européen* du CCBE et le *Modèle de code de déontologie des avocats européens* du CCBE, à savoir la confidentialité et la compétence professionnelle.

Confidentialité

Les avocats sont tenus de préserver la confidentialité de leurs communications avec leurs clients, des informations qu'ils reçoivent de ces derniers ainsi que des conseils qu'ils leur donnent. La confidentialité des communications entre un client et son avocat est protégée par le principe du secret professionnel qui s'applique également aux communications en ligne[19].

Le principe fondamental (b) de la Charte de la profession d'avocat européenne du CCBE concerne « *le respect du secret professionnel et de la confidentialité des affaires dont il a la charge* » *(et la nécessité qui en découle de faire des efforts raisonnables pour empêcher l'accès non autorisé ou illégal à des informations confidentielles)*.

Le point 2 de l'article sur la confidentialité du Modèle de code de déontologie du CCBE précise que : « *L'avocat est tenu au secret professionnel. Il s'agit d'un devoir qui peut également constituer un droit pour l'avocat.* ». Le point 4 du même article indique ce qui suit : « *Le secret professionnel s'applique à toutes les informations concernant un client ou à son dossier qui sont communiquées par le client à l'avocat ou reçues par l'avocat dans l'exercice de sa profession, quelle que soit la source de ces informations.* ». Le point 5 est libellé comme suit : « *Le secret professionnel s'applique également à tous les documents établis par l'avocat, à ceux remis par l'avocat à son client et à tous les échanges entre eux* ».

Compétence professionnelle

Les avocats sont tenus de mettre à jour et de maintenir leurs connaissances et leurs compétences professionnelles. Le principe fondamental (g) concerne *la compétence professionnelle de l'avocat (et la nécessité qui en découle de se tenir au courant des dernières*

[19] Pour plus d'informations sur la confidentialité des communications avocat-client, voir : 'La confidentialité des communications entre l'avocat et son client : un impératif pour protéger vos droits (2023)'.

évolutions technologiques et de leur effet sur la pratique de la profession et les obligations professionnelles de l'avocat).

L'article modèle sur les relations avec les clients, point 2.2, indique que : « L'avocat maintient ses compétences professionnelles à niveau au moyen d'une formation continue en matière juridique et dans les autres domaines en rapport avec sa pratique ». Le même point précise que : « *Une représentation compétente exige de la part de l'avocat qu'il possède les connaissances et les compétences juridiques et autres qui sont nécessaires pour lui permettre d'exécuter la mission qui lui est confiée par son client. L'avocat n'est en mesure d'y parvenir que s'il suit l'évolution rapide et continue de l'environnement juridique et technologique dans lequel il opère* ».

Le devoir de compétence de l'avocat ne se limite donc pas à la législation et à la réglementation, mais englobe l'obligation d'acquérir des connaissances sur un produit technique destiné à être utilisé dans le cadre d'activités professionnelles. Dans le contexte actuel, ces connaissances peuvent effectivement aider l'avocat à évaluer et à atténuer les risques liés à l'usage des services en nuage.

2. Comprendre les risques liés à l'usage de l'informatique en nuage

Il est important que les avocats analysent et évaluent les risques des produits et services spécifiques qu'ils ont l'intention d'utiliser. En fonction des résultats de cette évaluation, les avocats doivent mettre en œuvre les mesures nécessaires pour atténuer ces risques et demander des conseils supplémentaires si nécessaire. L'objectif d'évaluer et de gérer les risques liés à l'usage des services d'informatique en nuage vaut pour les cabinets d'avocats de toutes tailles, petits ou grands. Néanmoins, les sources de risques à évaluer, les détails de cette évaluation et les mesures possibles pour atténuer les risques dépendent à la fois du type et de la taille du cabinet d'avocats ainsi que du domaine d'activité du cabinet.

Les avocats devraient se tenir informés, par exemple en suivant des formations pertinentes, afin de maintenir à jour leurs connaissances sur les législations et réglementations applicables en matière d'informatique en nuage, de cybersécurité, ainsi que sur les obligations professionnelles dans ces domaines. Les barreaux devraient offrir aux avocats la possibilité de recevoir des informations et des formations pertinentes dans ces domaines.

3. Veiller au respect des règles déontologiques et de la législation en matière de protection des données

Les avocats devraient faire des efforts raisonnables pour examiner et comprendre à la fois les législations pertinentes et les obligations professionnelles nationales en ce qui concerne l'utilisation des données des clients, avant tout pour empêcher l'accès non autorisé ou illégal aux informations confidentielles et aux informations relevant du secret professionnel. Les avocats devraient en particulier vérifier s'ils sont autorisés, selon les règles déontologiques applicables, à stocker des données en dehors de leur cabinet et, le cas échéant, s'assurer que le fournisseur de services d'informatique en nuage n'est pas soumis à une juridiction dotée d'une législation de longue portée les obligeant à remettre les données d'avocats européens stockées sur un serveur dans le nuage à, le cas échéant, des autorités d'un pays non membres de l'Union européenne.

Les avocats doivent dès lors avoir une compréhension approfondie et respecter le règlement général sur la protection des données (RGPD), en se concentrant particulièrement sur les règles applicables aux responsables du traitement, aux sous-traitants, à la sécurité des données et aux droits des personnes concernées, ainsi que sur les règles relatives aux transferts et au stockage transfrontaliers de données.

En cas de violation de données, les avocats doivent notifier leurs clients, en consultation avec le délégué à la protection des données ou l'autorité nationale de protection des données, et les informer des mesures prises pour atténuer les dommages et prévenir les incidents éventuels.

4. Suivre les lignes directrices disponibles

Les avocats devraient suivre les lignes directrices fournies par les autorités de réglementation et les barreaux. Le CCBE a également publié un certain nombre de lignes directrices au cours des dix dernières années qui peuvent également être utiles aux avocats ayant recours à des services d'informatique en nuage. Il s'agit notamment de :

- Recommandations du CCBE sur la protection du secret professionnel dans le cadre des activités de surveillance (2016)
- Conseils du CCBE pour le renforcement de la sécurité informatique des avocats contre la surveillance illégale (2016)
- Guide du CCBE sur les plateformes en ligne (2018)
- Guide sur l'utilisation des outils d'intelligence artificielle pour les avocats et les cabinets d'avocats dans l'UE (2022)
- Lignes directrices du CCBE sur l'utilisation des outils de travail à distance par les avocats et les procédures judiciaires à distance (2020)
- Annexe aux lignes directrices du CCBE sur l'utilisation des outils de travail à distance par les avocats et les procédures judiciaires à distance : analyses des outils de vidéoconférence (2020)

Le CCBE a publié deux séries de lignes directrices sur le RGPD :

- Recommandations du CCBE pour la mise en œuvre du règlement général sur la protection des données (RGPD) qui fournissent une assistance aux barreaux pour se préparer aux effets des différences nationales affectant la façon dont les avocats doivent travailler pendant les efforts de mise en œuvre du règlement.
- Lignes directrices du CCBE sur les principales nouvelles mesures de conformité des avocats au règlement général sur la protection des données (RGPD) qui donnent un aperçu des principales nouvelles mesures de conformité que les barreaux peuvent recommander afin d'assurer la conformité avec les exigences énoncées dans le RGPD.

5. Garantir une sécurité de l'information adéquate

Les avocats, quelle que soit la nature de leur travail ou la taille de leur cabinet, doivent avoir mis en place les mesures de sécurité nécessaires pour protéger leur système informatique, y compris la sécurité de la communication avec les clients et le stockage des données de ces derniers.

Les avocats qui travaillent avec un grand nombre de clients privés et de petites sociétés devraient utiliser des outils compatibles avec les solutions qu'utilisent leurs clients. Ces cabinets devraient

prêter attention aux coûts cachés de l'interopérabilité et de la cybersécurité, tels que la perte de flexibilité quant aux produits informatiques qu'ils peuvent utiliser en raison de questions de sécurité, les difficultés d'utilisation des actifs informatiques que les clients fournissent, les coûts de configuration supplémentaire et de formation continue du personnel, les mises à jour régulières des fonctionnalités des services en nuage créant des ruptures dans la compatibilité, etc.

Les avocats devraient envisager de demander à leurs fournisseurs de se conformer aux normes de sécurité informatique applicables, par exemple celles élaborées par l'Organisation internationale de normalisation (ISO) ou les contrôles du système et de l'organisation (SOC) élaborés par l'American Institute of Certified Public Accountants :

- SO/IEC 27001:2022 - Sécurité de l'information, cybersécurité et protection de la vie privée - Systèmes de management de la sécurité de l'information - Exigences
- ISO/IEC 27017:2015 - Technologies de l'information - Techniques de sécurité - Code de bonnes pratiques pour les contrôles de sécurité de l'information fondés sur l'ISO/IEC 27002 pour les services en nuage
- ISO/IEC 27018:2019 - Technologies de l'information - Techniques de sécurité - Code de bonnes pratiques pour la protection des informations personnelles identifiables (PII) dans l'informatique en nuage public agissant comme processeur de PII[20]
- ISO/IEC 27036-4:2016 - Technologies de l'information - Techniques de sécurité - Sécurité d'information pour la relation avec le fournisseur, Partie 4 : Lignes directrices pour la sécurité des services du nuage
- SOC 2 - SOC pour les organismes de services : Critères relatifs aux services de confiance. La sécurité de l'information ne se limite pas aux seules mesures techniques et doit également inclure les politiques pertinentes et les pratiques organisationnelles visant à garantir la sécurité des informations et des données traitées par le cabinet.

En outre, les avocats doivent être attentifs à revoir périodiquement le statut de la certification (pour ISO) ou à demander de nouvelles attestations (pour SOC2) et à comprendre quelle documentation est utile pour leur évaluation des risques.

6. Connaître le fournisseur de services dans le nuage et les produits et services qu'il propose

Avant d'avoir recours à un service de stockage et d'autres services dans le nuage, les avocats devraient procéder à une évaluation des risques et sélectionner soigneusement leur fournisseur de services. Les avocats devraient en particulier effectuer une vérification diligente adéquate sur les garanties juridiques offertes par le fournisseur qu'ils ont l'intention d'engager pour la fourniture de services en nuage relevant du secret professionnel. Il existe plusieurs grands types d'informations à prendre en compte dans le cadre de cet exercice, qui sont énumérés ci-dessous. Ces informations peuvent figurer dans le contrat, les conditions générales du service, les avis de confidentialité, les avis relatifs aux cookies, ou dans des descriptions techniques, telles que dans les interfaces de programmation d'applications (API) ou d'autres documents destinés aux développeurs et autres spécialistes techniques. Les avocats doivent utiliser des sources d'information fiables pour sélectionner les produits ou services, notamment des sites web

[20] Au moment de la rédaction du présent document, entre juin et octobre 2024, la révision de la norme était en cours.

vérifiés, des sites web communautaires ou des forums de discussion, ainsi que les commentaires d'autres praticiens.

Les avocats doivent analyser les accords de niveau de service en termes de performance, de sécurité, de traitement des données et de respect de la vie privée et savoir qu'il existe trois types de contrats différents : le contrat d'adhésion, le contrat négocié et le contrat mixte.

Ce faisant, les avocats devraient accorder une attention particulière aux aspects suivants d'un service :

- **La disponibilité et qualité de l'assistance (service clientèle) :** plus la portée des services fournis par un fournisseur est large, plus un utilisateur qui se trouve être avocat devra compter sur les services clientèle de ce fournisseur. Dans ce cas, la réactivité et l'utilité du service clientèle d'un prestataire informatique est l'un des aspects les plus importants.
- **La stabilité financière et l'historique des services du fournisseur :** la vérification des rapports financiers publiés et les informations sur l'entreprise dans le registre des sociétés, la longévité de la même structure de propriété et l'ancienneté des services désirés du fournisseur (par exemple, par l'intermédiaire de services d'archives sur Internet).
- **La disponibilité et la qualité des informations sur les services fournis :** les fournisseurs choisis doivent disposer d'informations de bonne qualité sur leurs services, y compris les détails techniques (comme les fournisseurs d'infrastructures ou de plateformes en nuage, abrégées en IaaS et PaaS).
- **la transparence en ce qui concerne les sous-traitants utilisés :** les informations les plus utiles figurent généralement dans les conditions de protection de la vie privée dans la rubrique « sous-traitants ». L'emplacement physique du stockage des données figure généralement uniquement dans les clauses de confidentialité.
- **le respect des certifications, rapports et codes de déontologie pertinents de la part du fournisseur :** il est utile pour les avocats de vérifier ces éléments étant donné qu'il peut leur être difficile d'évaluer autrement la fiabilité des capacités techniques d'un fournisseur de services. Parmi les codes de déontologie, citons le *CSA Star Registry*[21], le Code de conduite Cloud de l'UE[22] et le code de déontologie de SWIPO[23].
- **l'identité des sous-traitants :** lorsqu'il n'est pas possible pour les avocats de vérifier la conformité à l'aide de ces codes ou certifications, les avocats doivent s'efforcer d'identifier :
    - les sous-traitants auxquels le fournisseur de services en nuage choisi fera appel ; et
    - l'étendue des services de ces sous-traitants.
    - Certains des sous-traitants peuvent disposer d'une certification ou d'un code pertinent, ce qui peut également donner une certaine assurance à l'avocat. Il est

[21] *CSA Star Registry*
[22] Code de conduite Cloud de l'UE : https://eucoc.cloud/en/home
[23] Code de déontologie relatif à la portabilité des données et au changement de service pour les services cloud d'infrastructure en tant que service (IaaS) Version : 2020, Date : 08/07/2020 : https://swipo.eu/wp-content/uploads/2020/07/SWIPO-IaaS-Code-of-Conduct.pdf.

toutefois important de noter que la conformité d'un sous-traitant par rapport à certaines parties du service total n'est pas toujours pertinente pour l'avocat[24].

Une autre approche, plus gourmande en ressources, consiste pour les avocats à vérifier manuellement quels types de prestations du code de déontologie donné sont présents dans les conditions générales publiées par le fournisseur de services en nuage. Même une conformité partielle basée sur les conditions générales publiques donne une image plus pertinente du fournisseur de services que l'absence totale d'un tel exercice. Si les conditions générales publiées ne comportent pas ces informations, les avocats doivent d'abord chercher à obtenir des informations sur ces questions directement auprès du fournisseur ou de son revendeur, et s'efforcer d'inclure toute assurance dans les conditions contractuelles conclues.

- **les conditions contractuelles :** lorsque les solutions techniques, les certifications ou les codes de conduite ne sont d'aucune utilité, les avocats doivent également vérifier les conditions contractuelles des services informatiques pour y trouver les informations suivantes :
    - des sauvegardes périodiques à des niveaux élevés de sécurité physique et logique ;
    - des mécanismes d'authentification pour l'accès aux informations pour les avocats du cabinet et les clients ;
    - le chiffrement des données stockées ;
    - le registre des accès aux données ;
    - un audit de sécurité par un tiers diligent ;
    - l'utilisation des données de l'utilisateur par le fournisseur : les données de l'utilisateur téléchargées ou générées dans un service en nuage utilisé en tant qu'avocat ne sont soumises à aucune notion de « propriété » dans l'UE, de sorte que les fournisseurs informatiques, en tant que responsables du traitement des données ou détenteurs de données, ne devraient pas pouvoir revendiquer de droits sur ces données ni les utiliser à d'autres fins que ce qui est simplement nécessaire pour la fourniture du service à l'avocat. Toutefois, compte tenu de la valeur de ces grands ensembles de données et de la difficulté de déceler un tel traitement, ce risque reste réel. Un tel usage peut parfois reposer sur des données anonymisées, l'anonymisation est rarement une solution permanente et sûre et peut dès lors comporter des risques considérables si elle est effectuée sur les données de l'avocat. C'est pourquoi les avocats devraient demander aux fournisseurs de services de leur garantir clairement dans leurs conditions qu'ils n'utiliseront pas les données de leurs clients à des fins autres que la fourniture de services (que ces données soient à caractère personnel ou non).
    - la juridiction et le règlement des litiges : bien que trivial pour les avocats, il convient tout de même de noter que, même pour les avocats, il peut être très difficile en pratique d'exécuter tout droit énoncé dans les conditions générales s'il est onéreux pour l'avocat en question de saisir les tribunaux ayant juridiction sur le contrat de services. En outre, de nombreux contrats SaaS prévoient un arbitrage obligatoire ou un règlement en ligne des litiges, ce qui est rarement avantageux du point de vue des petits cabinets d'avocats qui cherchent à obtenir réparation.

[24] Cela peut se produire par exemple lorsque le fournisseur informatique de l'avocat pourra transférer les données de son fournisseur sous-traitant à un autre, ce qui ne signifie pas que l'avocat pourra transférer ses données à un autre fournisseur.

- la limitation de la responsabilité : un autre point, plutôt banal, à partir duquel les avocats peuvent facilement comparer différents fournisseurs de services est la limitation de la responsabilité, ou plus probablement, le montant supérieur des dommages directs que le prestataire de services s'engage à payer en cas de rupture de contrat. Tout comme la plupart des produits informatiques, les prestataires de services en nuage tentent aussi généralement de limiter leur propre responsabilité en excluant certaines demandes ou catégories de dommages.
- toute pénalité ou crédit de service en cas de non-respect des objectifs de niveau de service : lors de la comparaison de services et de fournisseurs similaires, il conviendrait de privilégier ceux qui acceptent de fournir au moins un montant symbolique de pénalités ou de crédits de service s'ils ne remplissent pas les objectifs de niveau de service (tels que le temps d'indisponibilité, le temps de réponse, etc.) promis.
- la durée et la résiliation des services : avant de sélectionner un service, l'avocat devrait également comprendre comment le service utilisé peut être résilié à son initiative ou à celle du fournisseur. Les conditions doivent comporter une procédure de récupération et de migration des données en cas de résiliation du contrat. En outre, l'avocat doit préparer le plan de continuité des affaires du cabinet en fonction des délais de préavis de résiliation du fournisseur tel qu'indiqué dans le contrat. Cela s'applique également à la portabilité des données, les avocats devant être en mesure de récupérer les données dans un format lisible en vue d'une utilisation ultérieure ou à des fins de conformité (par exemple, fiscale).

7. Savoir où les données sont traitées

Les avocats doivent savoir où et comment les données de leurs clients sont traitées. Il s'agit notamment de vérifier la légalité et l'éthique du stockage des données en dehors de leur cabinet et de comprendre les différences entre les législations sur la protection des données des juridictions et de savoir si les transferts de données en dehors de l'UE sont autorisés et, le cas échéant, selon quelles conditions. Les avocats devraient donc connaître les mécanismes de transfert de données utilisés par leurs fournisseurs de services en nuage et les emplacements géographiques qu'ils utilisent pour stocker physiquement les données.

Mécanismes de transfert

Le RGPD prévoit plusieurs mécanismes de transfert qui sont décrits au chapitre V :

- les transferts avec décision d'adéquation[25] ;
- les transferts sans décision d'adéquation.

En l'absence de décision d'adéquation, d'autres mécanismes appropriés de transfert de données devraient être utilisés. Il s'agit notamment de règles d'entreprise contraignantes, de clauses types

[25] La liste des pays concernés par des décisions d'adéquation est disponible ici : https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en?prefLang=fr

de protection des données, de codes de conduite et de systèmes de certification, de dérogations au titre de l'article 49[26].

- Les clauses types de protection des données sont un modèle de mécanisme de transfert de données conçu principalement pour aider les responsables du traitement et les sous-traitants à faciliter légalement les transferts de données vers des pays tiers.
- Les règles d'entreprise contraignantes sont des règles et des politiques internes contraignantes et exécutoires pour les transferts de données au sein des entreprises multinationales.
- Les codes de conduite sont un outil de transfert élaboré par des associations représentant des catégories d'organisations dans un secteur donné.
- La certification est un nouvel outil pour les transferts de données vers des organisations qui ont été certifiées par des organismes de certification ou des autorités de protection des données dans l'UE/l'Espace économique européen (EEE). Cet outil est encore en cours d'élaboration.
- Les dérogations prévues à l'article 49 du RGPD autorisent les transferts de données dans des situations spécifiques, telles que l'exécution d'un contrat ou la défense d'une action en justice.

À la suite de la décision rendue dans l'affaire Schrems II, la Cour de justice de l'UE a souligné que les organisations pouvaient avoir besoin de mettre en œuvre des mesures supplémentaires en plus des garanties appropriées lorsqu'elles transfèrent des données à caractère personnel en dehors de l'EEE. La CJUE a indiqué que les responsables du traitement ou les sous-traitants, lorsqu'ils agissent en tant qu'exportateurs, doivent évaluer individuellement si les lois ou les pratiques du pays hors EEE, telles que celles imposant l'accès aux données, compromettent l'efficacité des garanties décrites à l'article 46 du RGPD.

Compte tenu des considérations exposées ci-dessus, les avocats devraient donc savoir quelles réglementations s'appliquent aux données stockées par leur cabinet et quelles mesures ils doivent prendre pour protéger tout le contenu relevant du secret professionnel et des obligations pertinentes en matière de protection des données.

Enfin, étant donné qu'il s'agit d'un domaine en évolution rapide et que les mécanismes de transfert de données applicables ont été contestés par le passé, les avocats devraient suivre régulièrement les mises à jour de la législation, de la jurisprudence et d'autres informations en la matière pour rester au fait de leurs obligations, ce qui comprend notamment les discussions géopolitiques sur la sécurité des données et l'ingérence potentielle des États, comme les portes dérobées ou les flux de données vers les États, même lorsque les entreprises prétendent traiter leurs données au sein de l'UE.

8. Savoir comment les données sont traitées

Compte tenu de l'omniprésence des services en nuage, les avocats devraient être conscients que même les applications et solutions les plus simples peuvent comporter le traitement de données par des tiers et leur utilisation ultérieure. Il peut s'agir d'assistants d'édition de texte, de traduction, d'édition d'images, etc. Si les présentes lignes directrices n'ont pas pour objet de

[26] Guide de l'EDPB sur les transferts internationaux de données

développer ces services, les avocats doivent néanmoins être conscients de ces possibilités de traitement et des conséquences qui en découlent.

9. Considérations sur la continuité de la pratique professionnelle

Lorsque les avocats stockent des données à distance, ils devraient s'assurer que les données peuvent être récupérées et que l'avocat en garde le contrôle. À cette fin, les avocats devraient mettre en place des mécanismes de gestion appropriés, notamment en définissant les catégories de données, en garantissant un accès local actualisé aux données essentielles et en disposant d'une connexion internet de secours.

Définir et catégoriser les données critiques

Les données devraient être classées en fonction de leur importance et de ce que l'on appelle l'objectif de perte de données maximale admissible (PDMA) : le temps maximum qui peut s'écouler entre deux sauvegardes de données avant qu'une perte de données ne devienne inacceptable du point de vue de l'entreprise. Il s'agit d'une décision que l'avocat doit prendre en toute connaissance de cause. Pour les services critiques, l'avocat a tout intérêt à comprendre s'il est possible d'effectuer des sauvegardes locales des données provenant des services en nuage et, si oui, comment effectuer ces sauvegardes locales automatiquement.

La définition des données critiques est quelque chose que les avocats eux-mêmes doivent définir et comprendre. Elle doit comprendre les données qui sont (i) soumises à des obligations de conservation par l'avocat, et (ii) sans lesquelles un avocat pourrait ne plus être en mesure de fournir une assistance efficace à un client. Une telle définition doit prendre en considération le service particulier rendu au client, toute promesse contractuelle faite au client concernant la conservation des données dans le contrat de mission, et les risques encourus par le client en l'absence d'un tel service juridique continu. La définition des données critiques doit également tenir compte du fait que certaines données peuvent être recréées à partir de sources tierces (y compris à partir des dossiers judiciaires ou en demandant aux clients de renvoyer les données qui ont été perdues).

Garantir un accès local actualisé aux données critiques

La question la plus importante pour un avocat est de savoir comment conserver une copie locale à jour des données clients les plus récentes dont il dispose. Cela pourrait inclure l'utilisation du courrier électronique de manière à garantir que des copies locales (caches) des boîtes de réception sont toujours disponibles (par exemple en utilisant IMAP, POP, .OST ou des offres de tiers pour les plus grands fournisseurs de services de courrier électronique). Compte tenu des remarques sur la confidentialité ci-dessus, les avocats devraient également se demander si ces tiers fournisseurs ont accès aux données qu'ils traitent.

Le même mécanisme est nécessaire pour d'autres stocks de données non liés à la messagerie, tels que les clients de bureau ou les serveurs sur site qui se synchronisent automatiquement avec le stockage en nuage. Il ne suffit pas d'avoir la possibilité technique de télécharger toutes ces données ; les avocats doivent s'assurer qu'ils peuvent disposer d'une copie des données critiques

en tenant compte de l'objectif de perte de données maximale admissible (PDMA) pour le cabinet. Il existe également un risque que la suppression de copies sur un appareil entraîne leur suppression sur d'autres appareils liés au même système de dossiers synchronisés (partagés). Ce risque est plus élevé lorsque plusieurs utilisateurs partagent l'accès au même dossier partagé.

Le problème se pose davantage si des solutions de gestion de cabinet ou des cas en ligne stockent ces données critiques. Par rapport aux solutions traditionnelles de stockage dans le nuage, ces outils sont vendus pour des marchés fragmentés avec relativement peu de clients, et même les outils les plus populaires peuvent ne pas prendre en charge des sauvegardes locales automatisées prêtes à l'emploi, et les solutions tierces feront également défaut. Il s'agit là d'un risque supplémentaire que les avocats devraient également prendre en considération.

On n'attend pas d'une solution de gestion de cabinet que toutes les données stockées dans ce système soient disponibles localement mais, à tout le moins, les données critiques devraient être disponibles de manière à ce que les experts informatiques locaux puissent techniquement recréer ou mettre ces données à la disposition des avocats pour un usage ultérieur dans le cas improbable d'une inaccessibilité soudaine et permanente du fournisseur de services. De simples promesses dans les conditions contractuelles ne peuvent pas remplacer l'accessibilité technique des données critiques.

Disposer d'un accès de secours à internet

Quelle que soit l'ampleur du recours à l'informatique en nuage, le maillon faible du point de vue de l'utilisateur final reste l'accessibilité à internet depuis les locaux du cabinet d'avocats. Grâce aux progrès des communications électroniques, d'autres moyens d'accès à internet pourraient être disponibles, comme la mise en place d'un autre fournisseur d'accès à large bande (utilisant un réseau de distribution et de base différent de l'original, et pas seulement un revendeur des mêmes lignes), ou un ou plusieurs accès à un réseau mobile sur lesquels le cabinet (ou automatiquement tout appareil utilisé par le cabinet) peut basculer en cas de besoin d'une connexion de secours. Les avocats devraient s'assurer qu'ils disposent d'un tel dispositif de secours en cas de besoin et tester ces changements au moins une fois par an. Il peut en outre être judicieux pour certains cabinets d'avocats de réfléchir à une solution en cas de panne d'électricité ou d'internet plus généralisée. Ils devraient également envisager de sauvegarder les données critiques sur un support physique déconnecté d'internet.

10. Disposer d'une couverture d'assurance appropriée

Étant donné que les avocats détiennent des données sensibles et confidentielles sur leurs clients, ils devraient envisager d'acquérir une couverture d'assurance cybernétique pour se protéger contre les coûts non désirés d'une violation de données, les coûts de restauration et des pertes subies par les activités du cabinet à la suite d'un cyber incident. En outre, les avocats devraient vérifier s'ils sont couverts ou non en cas de demandes de dommages et intérêts présentées par des tiers à la suite d'incidents cybernétiques tels que les attaques de logiciels rançonneurs (rançongiciels), ainsi qu'en cas de dommages résultant de problèmes matériels (qui sont souvent exclus de la police standard).

Les avocats devraient également envisager de négocier une clause contractuelle exigeant que le fournisseur de services d'informatique en nuage souscrive une assurance adéquate pour couvrir sa responsabilité dans le cadre de l'accord sur l'informatique en nuage.

III. Conclusion

L'informatique en nuage comporte de nombreux risques et enjeux tels que décrits dans ces lignes directrices, en particulier en ce qui concerne la confidentialité/le secret professionnel et la conservation des données. Le CCBE invite les barreaux à sensibiliser leurs membres à une plus grande vigilance et à adopter des précautions de haut niveau. Des garanties juridiques et techniques devraient leur être fournies par leurs fournisseurs d'informatique en nuage (c'est-à-dire une garantie de sauvegarde des données à long terme, etc.)

Les barreaux sont donc encouragés à soutenir les avocats sur les questions relatives à l'usage du nuage. Certains barreaux pourraient même envisager de développer des infrastructures et des services privés d'informatique en nuage pour leurs membres individuels et collectifs dans le respect des considérations ci-dessus. Il pourrait par conséquent leur être utile de procéder à une analyse d'impact[27].

[27] Le CCBE examine également la manière dont le changement climatique affecte les avocats et leur pratique. À cette fin, il élabore des lignes directrices pour aider les barreaux à examiner les effets potentiels du changement climatique sur l'exercice de la profession d'avocat, qui peuvent être pertinents dans le cadre du recours à l'informatique en nuage.