Image not found or type unknown

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

publié le **24/11/2012**, vu **3929 fois**, Auteur : Virtualegis

Le Conseil des barreaux européens (CCBE) entend mettre en garde la profession sur le danger que peut constituer le stockage par un tiers et dans un pays tiers, des données du Cabinet et invite les avocats européens à prendre toutes les précautions juridiques et techniques nécessaires, avant d’adopter le Cloud Computing

Le 7 septembre 2012, le Conseil des Barreaux de l’Union Européenne a publié une dizaine de **lignes directrices** à l’attention des avocats européens qui seraient tentés par le stockage de leurs données dans le Nuage en ayant recours *au **Cloud Computing**.* .

Après avoir brièvement exposé **les avantages** du *Cloud Computing* (réduction des coûts informatiques, de loyers, simplification de la gestion d’un cabinet, flexibilité du travail), le CCBE **insiste sur les risques de sécurité** que cette technologie fait courir à la profession d’avocat. Elle est actuellement, de nature à porter **atteinte au secret professionnel**, à la **confidentialité** et à la **conservation des données**.

Avec ce guide, le CCBE entend mettre en garde la profession sur le danger que peut constituer le stockage par un tiers et dans un pays tiers, des données du Cabinet et invite les avocats européens à prendre toutes les précautions juridiques et techniques nécessaires, avant d’adopter le *Cloud Computing.*

1. **Les risques mis en évidence par le CCBE**

Les principaux risques mis en évidence par le CCBE portent sur la protection des données, la violation des règles déontologiques dont le secret professionnel, et les difficultés liées à l’extraterritorialité.

La responsabilité de l’avocat en matière de respect du secret professionnel et la protection des données n’est pas strictement définie quant à la fiabilité et la sécurité du *Cloud Computing* sur lequel ils conservent les données de leurs clients. De même, le risque existe d’un **accès non autorisé par les employés ou sous-traitants du fournisseur** ou tout autre tiers plus ou moins bien intentionné. Quelle responsabilité pour l’avocat ?

Concernant **l’extraterritorialité**, le risque d’atteinte à la protection des données existe pour les Etats hébergeant, dotés d’une **législation moins rigoureuse que la réglementation européenne** en matière de données personnelles. Les serveurs du prestataire situés dans des pays moins

regardant que les pays membre de l'Union européenne sur la confidentialité, la propriété, la durée de conservation des données, l'identification des clients ou l'accès aux données en cas de rupture contractuelle, exposeront davantage les données à un risque.

2. Les pistes de réflexion préconisées par le CCBE

Il ressort des lignes directrices édictées par le CCBE que l'avocat qui envisage de recourir au *Cloud Computing* devra être guidé par deux principes : vigilance et transparence.

- Vigilance

L'avocat désireux de confier ses données à un tiers devra être vigilant au respect de ses obligations déontologiques et légales relatives notamment au secret professionnel et ce, dès avant la conclusion du contrat de *Cloud Computing* :

- en **évaluant le niveau de risque initial de sa propre installation** informatique,

- en réfléchissant au **type de modèle de service** qui répondrait convenablement aux besoins actuels et futurs du cabinet : SAAS ou IAAS, ce qui suppose que l'avocat ait une connaissance préalable des enjeux de traitement et de conservation des données,

- en réfléchissant au **type d'informations confiées** au prestataire (données sur les employés, données pénales, archives juridiques générales, etc.) et au niveau des mesures de protection à adopter en conséquence,

- en prêtant attention à **l'identité**, à la solvabilité **du prestataire**, à la **localisation des données**, aux **mesures de protections** mises en œuvre par le prestataire, au droit applicable,

- en évaluant les **mesures de sécurité techniques, physiques et organisationnelles** du prestataire au regard des normes nationales et internationales de gestion des risques informatiques (Norme ISO).

Cette **obligation de vigilance** se maintiendra également pendant l'exécution du contrat puisque l'avocat est invité à réfléchir à la stipulation des clauses prévoyant des solutions en cas de défaillance du prestataire.

D'une manière plus générale, la vigilance sera effectivement de mise s'agissant de la récupérabilité des données. La réversibilité et la réplication des données en cas de défaillance du prestataire et d'une manière générale la disponibilité des données devront faire l'objet d'une négociation préalablement à la conclusion du contrat.

- Transparence

Copyright © 2025 Légavox.fr - Tous droits réservés

Le CCBE **invite l'avocat à informer son client de l'utilisation d'un service de *Cloud Computing***. Il propose que cette information figure de façon détaillée, dans les contrats de services juridiques. Le CCBE souligne à cet égard que certains Etats européens ont d'ores et déjà prévu que le consentement éclairé du client devait être requis pour le stockage de ses données personnelles.

Le client devrait ainsi être tenu **informé** de la conclusion d'un contrat de *Cloud Computing*, **des normes** juridiques applicables en matière de protection des données, **de droit à la vie privée et de secret professionnel dans le pays où les données sont stockées**.

Ces lignes directrices du CCBE permettent de s'interroger sur l'opportunité d'encadrer le stockage des données des clients de profession libérale. *Quid* de la création d'un *Cloud* privé, propre à chaque Barreau et, qui permettrait à tout avocat, quelque soit la taille de son cabinet, de bénéficier des vertus technologiques du *Cloud* ?

Pascal ALIX et Gwendoline PERFETTI, Avocats à la Cour

Cabinet VIRTUALEGIS : www.virtualegis.eu

Copyright © 2025 Légavox.fr - Tous droits réservés