CCBE GUIDELINES
ON THE USE OF CLOUD COMPUTING SERVICES BY LAWYERS

Conseil des barreaux européens – Council of Bars and Law Societies of Europe
association internationale sans but lucratif
Avenue de la Joyeuse Entrée 1-5 – B 1040 Brussels – Belgium – Tel.+32 (0)2 234 65 10 – Fax.+32 (0)2 234 65 11/12 – E-mail ccbe@ccbe.eu – www.ccbe.eu

CCBE guidelines on the use of cloud computing services by lawyers

TABLE OF CONTENTS

I. INTRODUCTION

1. Scope of the guidelines

This paper is intended to create more awareness about the various risks associated with cloud computing. As such, the guidelines in Part II of this paper are addressed to the CCBE's member bars and law societies drawing attention to the issues which are likely to be faced by individual lawyers in making informed decisions when advising on or considering the use of cloud computing services.

2. Cloud computing

Cloud computing is a general term for IT infrastructure that involves storing and processing data and software remotely in the cloud provider's data centre or interlinked centres, accessed as a service by using the Internet. According to the US National Institute of Standards and Technology (NIST), cloud computing enables omnipresent, convenient, on-demand network access to a shared pool of configurable computing resources, such as networks, servers, storage, applications and services, that can be rapidly released with minimal management effort or service provider interaction[1].

3. Cloud computing on the European Commission agenda

The need to develop an EU-wide strategy on cloud computing has been highlighted in the European Commission Digital Agenda for Europe. The three broad areas to be addressed in this context in order to ensure that Europe maximises the benefits from cloud computing include:

- The legal framework: this concerns data protection and privacy, including the international dimension. It also concerns laws and other rules that have a bearing on the deployment of cloud computing in public and private organisations.
- Technical and commercial fundamentals: the aim is to extend the EU's research support and focus on critical issues, such as security and availability of cloud services.
- The market: pilot projects will be supported aiming at cloud deployment. Really to harness the power of public procurement, the Commission will engage with public-sector partners in the Member-states and at regional levels to work on common approaches to cloud computing.

As the Commission reports, work has already started in some of these areas, including a public consultation in 2011 to which the CCBE responded[2].

4. Cloud computing for lawyers: benefits and risks

Law firms as well as other businesses use cloud computing for many reasons. The reduction of costs constitutes one consideration. Cloud computing might involve decrease in expenses to purchase servers and software or to hire IT staff to maintain the servers. In addition, since many cloud computing applications include access from anywhere, an easy setup of off-site work can save rent and travelling costs as well as facilitate joint working amongst the offices of multi-location law firms.

Moreover, cloud computing can simplify computing work for many law offices. For firms with an existing IT infrastructure, cloud-based software programmes can reduce IT complexity. Likewise, for law practices starting out, with no pre-existing software systems in place, it is relatively simple matter to create an effective practice management system from the ground up using cloud-based software programmes.

Cloud computing systems usually provide increased flexibility for the end user, since cloud computing services are accessed via an Internet connection from anywhere at any time. Similarly, unlike desktop or server-based software systems, cloud-based platforms can be used on any type of computer or

1 P. Mell and T. Grance, The NIST Definition of Cloud Computing, National Institute of Standards and Technology, US Department of Commerce (January 2011).
2 CCBE Response regarding the European Commission public consultation on cloud computing.

Internet-enabled device, using any type of operating system. As long as the users can access the Internet, they can access files stored on the cloud. As such, cloud computing might enable lawyers to provide their services in novel and more efficient ways, to the benefit of their clients.

Nevertheless, alongside many significant benefits, cloud computing also brings its own set of risks and challenges for lawyers, most significantly in relation, first to questions of data protection, second, to professional obligations of confidentiality and, third, to other professional and regulatory obligations incumbent on the lawyer. Though the first and second of these areas are closely related, they are not necessarily identical. The lawyer will also require to be sensitive to purely commercial risks to which he may be exposed, for example by a temporary unavailability of his cloud service causing disruption to his business.

The essence of cloud computing is the use of a third party, remote provider for computing services including the storage of data, as opposed to the use of computers or servers on the premises of the user or wholly under the user's control. The Cloud provider will often own or rent from other providers huge data centres which, in the case of the largest cloud providers may be interlinked to form a network of servers some of which may be located, in countries outside the EEA, where different and, it may be, a lower standard of data protection may apply. In a few cases, such centres may be located in countries which do not fully respect the rule of law. Furthermore, where there is a network of cloud servers, data may be disaggregated and stored on different servers (even in different countries) and even be constantly migrating amongst those servers. In most cases, even the controllers of such networks will be unaware of where, precisely, in the network an item of data may be stored at any given time. These circumstances clearly raise specific issues and possible concerns for the legal profession relating to standards of data protection and potential theft, loss or disclosure of confidential information.

The most direct concerns of lawyers arising out of cloud computing include[3]:

Issues relating to professional secrecy and data protection:

- Lawyers‘ responsibility might need to be clarified concerning the reliability and the safety of the Cloud on which they store their Clients‘ data
- Cloud computing might necessitate clarification of the extent to which lawyers need to obtain client’s consent before using cloud-computing services to store or transmit confidential information.
- Data stored in a cloud computing environment might be susceptible to risks of unauthorised access either physically through unauthorised access to the premises in which the servers are located or electronically, either by the provider’s employees or sub-contractors, or by outside parties, for example hackers, via the Internet.

Issues relating to extraterritoriality:

- Cloud computing might involve data processing on servers in countries which have fewer or less effective legal protection mechanisms for electronically stored information than are mandated in the EU/EEA and which do not fall within the EU regulatory regime. Cloud computing providers might be subject to local rules obliging them to hand over European lawyers’ data stored on a cloud server to, as the case might be, non-EU national authorities.
- An additional risk factor is long-arm foreign legislation which might seek to impose obligations to disclose data upon request to national authorities, not only upon home state companies providing cloud services, but also on foreign companies which are ultimately owned by home state companies. In this respect, cloud computing might be subject to unclear procedures governing response or refusal of the provider to government requests for access to information.

Issues relating to (local) deontological/regulatory requirements:

3 Several of these issues were identified in the following papers: The Law Society of Scotland’s Cloud Computing - Advice for the profession (2012) and American Bar Association‘s Commission on Ethics 20/20 Working Group on the Implications of New Technologies Issues Paper Concerning Client Confidentiality and Lawyers’ Use of Technology (September 20, 2010).

- Problems might also arise out of the fact that there may be diverging and/or conflicting local requirements of national bars or law societies to which lawyers need to adhere with regard to the handling of confidential data.

Issues relating to contracts with cloud computing service providers:

- Cloud computing might be subject to unclear policies regarding ownership of stored data.
- Cloud-computing providers might fail to back up data adequately and/or provide permanent availability of their Cloud services.
- Cloud computing might be subject to insufficient data encryption.
- Cloud computing might be subject to unclear policies for notifying customers of security breaches.
- Cloud computing might be subject to unclear policies regarding the duration of data storage.
- Cloud computing might be subject to unclear policies for data destruction in cases when a law firm no longer wishes the relevant data to be available on the cloud computing server or when it wishes the data to be transferred to another law firm.
- Cloud computing might involve problems relating to data access using easily accessible software in the event that a law firm terminates its relationship with the cloud-computing provider or when the provider changes or goes out of business.

5. CCBE guidelines on cloud computing

As outlined above, cloud computing provides a constructive alternative to traditional IT infrastructure systems for lawyers. However, alongside many significant benefits, it also entails a set of risks and challenges affecting lawyers' ability to adhere to their legal obligations as data controllers under the Data Protection Directive, to their professional codes of conduct, particularly as regards obligations of client confidentiality, and to their responsibilities under the regulatory regimes to which they may be subject, for example in maintaining accounting records which might be inspected by their regulator, or providing for continuity of business in the event that their law firm ceases to be able to provide its services.

It is imperative that lawyers, when considering deploying cloud computing in their offices, take necessary steps to ensure that client data is protected, that client confidentiality is maintained and that the concerns identified in paragraph 2 above are adequately addressed. Nevertheless, like other consumers, lawyers will often not know enough to be certain that security measures are sufficient. Within this context, the CCBE has developed this set of guidelines on the use of cloud-computing services by lawyers. These guidelines are intended to make lawyers more mindful of the various risks associated with cloud computing and to assist them in making informed technology decisions.

II. CCBE GUIDELINES ON THE USE OF CLOUD COMPUTING SERVICES BY LAWYERS

National Bars and Law Societies, in advising those of their members who are considering deploying cloud computing in their offices should seek to draw to their attention the following considerations:

A. Data protection laws and professional secrecy principles

As a general rule, data protection laws and professional secrecy principles should be taken into account by lawyers as a primary step when considering using cloud computing services. Particularly, lawyers should verify whether they are allowed under the rules of their home state bar or law society to store data outside their law firm and, if so, ensure that the cloud computing service provider is not subject to a jurisdiction with long-arm legislation obliging them to hand over European lawyers' data stored on a cloud server to, as the case might be, non-EU national authorities. Lawyers may wish to consider whether, in view of these concerns, it might not in any given case, be more appropriate to

use a cloud service provider established within the EEA and (wherever situated) so far as practicable not subject to such long-arm jurisdiction.

B. Preliminary examination of cloud computing services

Law firms are invariably engaged in processing different types of data to which various requirements in terms of handling and protection may apply, subject to the overriding obligation of professional confidentiality/secrecy. Lawyers considering using cloud computing services should first think about the type of service model, which would suitably fulfil current and future needs of their offices. When using Cloud Software as a Service (SaaS)[4] or Cloud Infrastructure as a Service (IaaS)[5] laywers will have to assure that both of them include processing and storage of data which may well include personal data and sensitive personal data, as well as information protected by client confidentiality. Lawyers have thus to be informed and aware of these considerations when processing data externally. Establishing encryption procedures of data in data transmission and storage should also be considered.

In these circumstances, if a lawyer intends to use cloud computing, the first decision to be made will be whether to adopt the SaaS or the IaaS models.

Further, cloud computing services may be provided by a public cloud provider or a private cloud provider. A public cloud provider is one who offers his services to all, whereas a private cloud provider will typically be owned and/or controlled by a small group. For example, in some Member States, lawyers have themselves grouped together to form private clouds. The public/private cloud distinction may be highly pertinent in an evaluation of which provider presents the lower risk factor, for example in relation to the possibility of storage of data on servers situated outside the EEA or data which may be the subject of long-arm jurisdiction. The use of a public cloud should by no means regarded as always being unsuitable, provided that the lawyer has first done due diligence on the provider itself, on the security of the data centre used by the provider and on the detail of the Service Level Agreement. In the event that such due diligence reveals concerns, it may well be that providers (particularly small and medium sized ones) would be prepared to adapt their services and/or negotiate contract terms so as to address those concerns.

Before contracting, a lawyer, as the end user of the cloud service, should verify:

[a] the experience,

[b] the reputation,

[c] the specialisation,

[d] the registered address and location of the cloud computing service provider.

In addition, a separate verification of the following should be conducted:

[a] the providers' solvency, reliability, ownership and capital adequacy,

[b] any potential conflicts of interests,

[c] risks of any misuse of the stored information,

[d] exact localisation of the storing servers,

[e] so far as practicable, the security both physical and electronic of the servers and the data centre in which they are located,

---

4 SaaS (Cloud Software as a Service): a provider delivers, via the web, various application services and makes them available to end-users. These services are often meant to replace conventional applications to be installed by users on their local systems; accordingly, users are ultimately meant to outsource their data to the individual provider. This is the case, for instance, of typical web-based office applications such as spreadsheets, text processing tools, computerized registries and agendas, shared calendars, etc.; however, the services in question also include cloudbased email applications. Source: Article 29 Data Protection Working Party, Opinion 05/2012 on Cloud Computing

5 IaaS: a provider leases a technological infrastructure, i.e. virtual remote servers the end-user can rely upon in accordance with mechanisms and arrangements such as to make it simple, effective as well as beneficial to replace the corporate IT systems at the company's premises and/or use the leased infrastructure alongside the corporate systems. Such providers are usually specialized market players and can rely actually on a physical, complex infrastructure that often spans over several geographic areas.Source: Article 29 Data Protection Working Party, Opinion 05/2012 on Cloud Computing.

[f] the applicable civil, criminal and public laws and regulations

C. Pre-evaluation of data sensitivity

Law firms are invariably engaged in processing different types of data to which various requirements in terms of handling and protection apply. Any decision to store information on the cloud server should be necessarily accompanied by considerations on the type of information (employee data, criminal data, general legal archives, etc.) and the level of protection measures that should be adopted accordingly.

D. Assessment of security measures

Any assessment of cloud-service providers should involve evaluation of adopted technical, physical and organisational security measures in accordance with national and international IT-risk-management standards, such as ISO 27001:2005 (security management) and ISO 9001 (quality management) Certificates issued by acknowledged IT auditors could also serve as a test criterion.

When applicable, a lawyer would also need to assess reliability of his own in-house security standards by setting up ICT rules, providing information and training staff. Since effective password management is rarely accomplished in its entirety by law firms, tokenisation or introduction of electronic ID-card registration on desk should be considered.

In general, a lawyer should always consider obtaining professional support and advice when selecting and monitoring cloud-service providers.

E. Comparing existing in-house IT infrastructure with cloud services

When evaluating cloud services, lawyers should make a comparison with their current in-house IT infrastructure. Such evaluation would enable the law firm to decide if switching to a separate cloud service might reduce or increase risks.

F. Assessment of ability to recover data in the event of the failure of the cloud service provider, failure of the law firm or contractual dispute between the provider and law firm

A lawyer will not wish to suffer business disruption in the event of the failure of his cloud service provider. Additionally, in many jurisdictions, lawyers are under professional and regulatory requirements to have client data and other material which may not be personal or client data (such as their firm's accounting records) available for inspection by appropriate professional and national regulatory bodies. If such material is not able to be made available when required by such authorities, whether by reason of the failure of the cloud service provider, the failure of a lawyer's own business (leading to a breach or the termination of the contract with the cloud service provider) or by reason of a contractual dispute with the cloud service provider which might give rise to a lien or right of retention by the provider over the lawyer's data, then that may expose the lawyer to a finding of professional misconduct or to the commission by the lawyer of a regulatory offence, as a result of his not having produced the data or other material. Such offence or misconduct may be continuous or repeated so long as the inability to produce the material continues.

Therefore, in evaluating cloud service providers, a lawyer should assess his own vulnerability to adverse professional or regulatory consequences arising through such an unavailability of data. He should consider whether it is necessary to seek to negotiate appropriate contractual terms to ensure such continued availability, even in the event of a contractual dispute or failure of either the provider or his own law firm. He may also require to assess whether it is necessary also to seek technical means to overcome such unavailability. For example, a contractual right to recover data may be of limited utility if the data is in a form which is not easily readable. It may be necessary to ensure the continued availability of the software required to read the data, for example, by means such as the licence of the relevant software being held in escrow for the benefit of the lawyer.

G. Contractual precautions

It is important to at least consider the following aspects:

[a] scope of service,

[b] system availability,

[c] deadlines for error corrections and removal of malfunctions,

[d] contractual fines for non-performance and delays (if enforceable under the applicable national laws),

[e] changes in service requirements,

[f] service provider's obligation to system adaptations required due to regulatory or legislative amendments,

[g] exclusion of engagement of sub-contractors without prior consent,

[h] licenses, particularly assurance that the software used by the provider has been properly licensed to it,

[i] ownership of data stored and exclusive right of access,

[j] data protection agreements, in particular if and to the extent required by applicable national laws[6],

[k] security measures and responsibility,

[l] non-disclosure obligations,

[m] monitoring and reporting,

[n] technical documentation, process documentation and user/system administrator documentation,

[o] right to control and audit, including standard certifications,

[p] back-up, disaster recovery contingency plan,

[q] provision for Software-ESCROW in case of insolvency or business incapability of the cloud-service provider,

[r] location of servers - national, EEA or outside of the EEA but with the European standards in respect to privacy and confidentiality,

[s] insurance, guarantees, warranties, damages,

[t] term, termination,

[u] end of service and exit-management provisions, including on transmission and deletion of data,

[v] mediation, conciliation and/or arbitration,

[w] applicable law and jurisdiction.

H. Contingencies

Attention should always be paid to the fact that cloud-service availability depends on an uninterrupted network connection. The lawyer should consider whether it may be necessary to have an alternative or back-up means of connecting to the internet in the event that his primary connection should fail.

6 For example, such as under Section 11 of the German Data Protection Act.

I. Transparency

In order to ensure transparency of legal services, a lawyer might consider informing his future clients that the law firm uses cloud computing services. This could be achieved by inserting the information into the general conditions of any legal-service agreement, subject to changes as negotiated with individual clients. This formula would enable the giving of more detailed information on cloud computing exclusively upon individual request. It should be noted that there may be certain jurisdictions where client consent is necessary.

The insertion of information into the general conditions of a legal-service agreement would be particularly advisable in cases when a law firm uses services of a cloud provider with servers located in a different jurisdiction. In such a case, a lawyer might need to obtain informed consent from his client to store confidential data on such servers. Information on the cloud-service provider as well as legal standards on data protection, privacy law and professional privileges of lawyers in a country where the servers are located should be provided to the client.

J. General consideration

Cloud computing involves many risks and issues as outlined in these guidelines, particularly with regard to confidentiality/legal professional privilege and data retention. The CCBE invites Bars and Law Societies to increase awareness among their members for greater vigilance and to adopt high-level precautions. Legal and technical safeguards should be provided to them by their cloud computing providers (i.e. long-term data backup guarantee, etc.).

In practice, it might not always be possible for individual lawyers to satisfy all these considerations. Bars and law societies are therefore encouraged to determine mechanisms to facilitate lawyers to be able to comply with these guidelines, such as developing in-house cloud computing infrastructures in compliance with the above mentioned considerations. In this case, they may wish to carry out an impact assessment.