CCBE RESPONSE REGARDING THE EUROPEAN COMMISSION PUBLIC CONSULTATION ON CLOUD COMPUTING

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 response regarding the European Commission Public Consultation on Cloud Computing

The Council of Bars and Law Societies of Europe (CCBE) represents around 1 million European lawyers through its member bars and law societies from 31 full member countries, and 11 further associate and observer member countries. The CCBE responds regularly on behalf of its members on policy issues which affect European citizens and lawyers.

In this submission, the CCBE is responding to the European Commission's request to obtain input from interested parties on the needs, barriers and opportunities of the use and provision of cloud computing. Instead of responding to the specific set of questions, the CCBE wishes to draw the Commission's attention to a number of more general issues and points of concern from the legal profession's point of view.

Clouds for lawyers

Law firms, in line with other businesses, are using or planning to use cloud computing for many reasons, as follows:

- the reduction of costs;
- the simplification of computing system for many law offices;
- the increased flexibility for the end user, since cloud computing services are accessed via an Internet connection from anywhere, at any time.

Despite these benefits, cloud computing also entails major risks for lawyers, which are mostly related to the security of client information. Under this system, instead of storing data on their own computer, or server, lawyers and law firms use a third party storage provider for reasons of efficiency. The storage provider normally owns huge data centres or even rents the data centres from another party which may be located, for instance, in a country outside the EU where data protection and the rule of law might be minimal. Hence, the data can be hosted at the servers of a third party, which could be on his/her servers or of another third party, as data can be transferred from one server to another server in seconds. Moreover, part of the data could be on one server and the other part on another server. These circumstances clearly raise specific issues and possible concerns for the legal profession relating to potential theft, loss, or disclosure of confidential information.

By way of background, lawyers have an ethical duty to protect client data. This duty expresses itself in different ways in various Member States and legal systems – sometimes called professional secrecy, sometimes legal professional privilege, or by some other title. But the duty, which is also a fundamental right of the client, is a unifying feature of the legal profession in all Member States, and recognised as such in jurisprudence of the European Court of Justice and EU directives. Lawyers have to abide by stringent national rules to comply with this duty which, in some countries, would limit or forbid the possibility of lawyers bound by professional secrecy to use a third party data storage provider.

Following on from these duties, the most direct concerns of the CCBE arising out of cloud computing include[1]:

- cloud computing providers might be subject to local rules obliging them to hand over European lawyers' data on a cloud service to (non-EU) national authorities;
- unauthorised access to confidential client information by a provider's employees (or sub-contractors) or by outside parties (e.g., hackers) via the Internet;

1 American Bar Association (ABA), ABA 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.

- the storage of information on servers in countries with fewer legal protections for electronically stored information;
- a provider's failure to back up data adequately;
- unclear policies regarding ownership of stored data;
- the ability to access the data using easily accessible software in the event that the lawyer terminates the relationship with the cloud computing provider or the provider changes businesses or goes out of business;
- the provider's procedures for responding to (or when appropriate, resisting) government requests for access to information;
- policies for notifying customers of security breaches;
- policies for data destruction when a lawyer no longer wants the relevant data available or transferring the data if a client switches law firms;
- insufficient data encryption;
- the extent to which lawyers need to obtain client consent before using cloud computing services to store or transmit the client's confidential information.

It is imperative on lawyers, when it comes to storing information in "the cloud", just as with any other form of storage, to take steps to ensure that confidential client data is protected. Nevertheless, like other consumers, lawyers will often not know enough to be certain that security measures are sufficient. In this respect the CCBE considers that its member Bars and Law Societies in the various Member States have a role to play to provide lawyers with access to resources that educate, with an aim of leaving lawyers in a position to make informed technology decisions. In fact, at this moment the CCBE is about to develop a set of guidelines about how to avoid risks related to cloud computing. **However, the CCBE believes that also major responsibility rests on the shoulders of the EU to ensure the maximum level of data protection and to provide model terms and conditions that could be incorporated into agreements between cloud computing providers and their clients.**

Legislative Framework

The CCBE certainly believes that updates to the current EU Data Protection Directive could further facilitate cloud computing while preserving the level of protection. In its response to the Commission communication on a comprehensive approach on data protection in the European Union[2], the CCBE already expressed its support to review EU's legal framework regarding data protection in order to make it more coherent and to take into account the new challenges of the information society. Cloud computing is clearly one of these new challenges which, besides offering considerable opportunities, also raises difficult data protection and jurisdiction issues. **In this respect, the CCBE reiterates its call upon the EU institutions to take into account the specific situation of the lawyer defending the interests of one specific party, being bound by stringent deontological and legal rules, and to ensure that lawyers' professional secrecy prevails over all data protection rules.**

In addition, given the international character of cloud computing, **the CCBE encourages the Commission to engage in negotiating binding international agreements with non-EU states so as to increase internationally the extent of the protection of personal data.** On this point, the CCBE is greatly concerned about recent information suggesting that, on the basis of the Patriot Act, the US authorities can access personal data stored in the EU by companies with headquarters in the US.[3] If this information is correct, the CCBE strongly urges the Commission to remedy this situation, and **ensure that EU data protection rules can be effectively enforced and that third country legislation does not take precedence over EU legislation.** If not, the CCBE calls for new mechanisms to guarantee that EU lawyers can exclusively use cloud computing providers that will keep their data in the EU. Consequently, it is essential to introduce a clause in IT contracts putting an

2 European Commission Communication COM(2010) 609 final on "A comprehensive approach on personal data protection in the European Union".

3 http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+WQ+E-2011-006901+0+DOC+XML+V0//EN and http://www.zdnet.com/blog/igeneration/microsoft-admits-patriot-act-can-access-eu-based-cloud-data/11225.

obligation on cloud computing providers to locate and make accessible their servers only within European Union territory.

It is also essential to introduce mechanisms to separate lawyers' data from other data.

Generally, the essential elements that need to be considered when negotiating international agreements are:

- that general terms and conditions of permissibility of treatments laid down in European regulations are complied with (Chapter II Directive 95/46/CE);
- that the person concerned can defend his/her interests in case of non-compliance with these principles (right of access, correction and recourse to the courts to seek legal remedies);
- that an independent monitoring body is provided for.

More generally, the use of cloud computing by lawyers presupposes the maximum levels of security requirements.

As stated before, the CCBE also believes that it is useful if the **EU institutions would develop model terms and conditions that could be incorporated into agreements between cloud computing providers and their clients**. Such terms and conditions should address:

- the ownership and physical location of stored data;
- the provider's backup policies;
- the accessibility of stored data by the provider's employees or sub-contractors;
- the provider's compliance with particular national laws governing data privacy (including notifications regarding security breaches);
- the format of the stored data (and whether it is compatible with software available through other providers);
- the type of data encryption;
- policies regarding the retrieval of data upon the termination of services;
- performance levels (continuity of access).

In addition to this, the CCBE would greatly **welcome the Commission urging cloud computing service providers to adhere to the maximum level of technological security**. Such high level security could collectively form a standard for the storage and transmission of confidential client data across a variety of organisations that employ cloud computing technology and be included in any guidelines the Commission chooses to make with respect to best practices and cloud computing.

CCBE Recommendations

The CCBE therefore urges the European Commission to take into account the following guidelines in its work on a European Cloud Computing Strategy:

1. to guarantee absolute protection for legal professional privilege as a safeguard for citizens' right to privacy.
2. to ensure the maximum level of data protection;
3. to take into account the specific situation of lawyers by considering their stringent deontological and legal rules;
4. to engage in negotiating binding international agreements with non-EU states so as to increase internationally the extent of the protection of personal data;
5. to ensure that EU data protection rules can be effectively enforced and that third country legislation does not take precedence over EU legislation;

6. to develop model terms and conditions that could be incorporated into agreements between cloud computing providers and their clients;
7. to urge cloud computing service providers to adhere to the maximum level of technological security requirements.