CCBE RESPONSE TO THE COMMISSION COMMUNICATION ON A COMPREHENSIVE APPROACH ON DATA PROTECTION IN THE EUROPEAN UNION

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 to the Commission communication on a comprehensive approach on data protection in the European Union

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 views on how to address the new challenges for personal data protection (e.g., fast developing technologies, globalisation) in order to ensure an effective and comprehensive protection to individuals' personal data within the EU, as highlighted in the Communication COM(2010) 609 final on "A comprehensive approach on personal data protection in the European Union".

CCBE supports and profoundly respects the fundamental right to protection of personal data, including the right of respect of privacy and that of confidentiality of communications. The current legal framework is however not up to date, not coherent, and does not take into account the new challenges of the information society. In this respect CCBE welcomes the initiative of the European Commission to review the legal framework.

In this document, CCBE shares its views on data protection seen from the perspective of the European lawyer. CCBE also refers to its earlier position paper "CCBE position on the legal framework for the fundamental right to protection of personal data" of 4 January 2010.

1. The profession of a lawyer

The profession of a lawyer comprises to a great extent the processing of data, especially of personal data. This does not only concern the client's data, but also that of the opponent and possibly affected third parties, e.g. witnesses, rival applicants in a promotion process in civil service law procedures, family members in divorce cases, or employees affected by a dismissal on the basis of social criteria. Within the legal framework, the lawyer is obliged to protect the interests of his client unilaterally, both on the basis of the concluded contract and the deontology of the legal profession.

There is a good reason why lawyers have been subject to professional secrecy for decades and centuries, as professional secrecy protects the client themselves and, moreover, assures a reasonable protection of interests for all concerned. Hence, professional secrecy serves both as protection of the client themselves and the legal order in an objective way. Legal professional secrecy essentially also covers the data of the opponents and any third parties which the lawyer might learn during the exertion of his profession. The lawyer stores this data solely in line with his professional activity and hence in line with the interests of his client.

This specific situation distinguishes the legal profession from nearly every other individual subject to data protection rules. This is notably valid in view of the fact that the lawyer protects external interests and stores personal data of different persons. The existing EU data protection directive does not settle in a clear way the conflict situations arising, and hence does not serve the legal protection of the interests served by a lawyer. This should be taken into account when reviewing the legal framework.

2. Suggestions for enhancing the data protection legal framework

Taking into account the specific professional situation of the lawyer, the following regulating rules are necessary.

a) The lawyer's professional secrecy must prevail over all data protection rules.

Lawyers' professional secrecy must prevail over all data protection rules. No data protection rule shall breach this professional secrecy which should be an unconditional priority of legal practice of lawyers. Furthermore, the data protection rules shall not oblige lawyers to respect third-party interests. In this respect, lawyers' professional secrecy constitutes a specific data protection rule. This implies a clear regulation providing that the processing of client-specific data of lawyers is only subject to lawyers professional secrecy (which is generally not limited by time) and not to any other data protection rules. However, the processing of other data could also be subject to general data protection rules.

b) Supervision of compliance by a special independent authority

The supervision of compliance with the data protection rules shall be exclusively accomplished by a special independent authority that is familiar with the specificities of the legal profession. A special independent authority is solely able to take into consideration the specific interests of lawyers in taking a decision. In Germany, such a control is already performed by the regional member bars of the Bundesrechtsanwaltskammer (BRAK). The EU Data Protection Directive must contain clear rules that enable each member state to establish a special control authority in line with their own specific state law.

Ensuring the independence of the control authority with regards to lawyers is a prerequisite to avoid conflicts of interest resulting from an involvement of the said authority in the procedure e.g. as the authority initiating the administrative act in the administrative, social or transportation sector.

As for independence on the subject of the EU data protection directive, the CCBE would like to call to mind that the European Court of Justice stipulated in its judgment of 9 March 2010 concerning the *European Commission v Federal Republic of Germany* that "the independence of the supervisory authorities, in so far as they must be free from any external influence liable to have an effect on their decisions, is an essential element in light of the objectives of Directive 95/46. That independence is necessary in all the Member States in order to create an equal level of protection of personal data and thereby to contribute to the free movement of data, which is necessary for the establishment and functioning of the internal market".[1] In its conclusion on the same judgment the Court therefore declared that "by making the authorities responsible for monitoring the processing of personal data by non-public bodies and undertakings governed by public law which compete on the market (öffentlich-rechtliche Wettbewerbsunternehmen) in the different Länder subject to State scrutiny, and by thus incorrectly transposing the requirement that those authorities perform their functions 'with complete independence', the Federal Republic of Germany failed to fulfil its obligations under the second subparagraph of Article 28(1) of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data".

Having regard to these considerations the CCBE believes that with regards to lawyers, the Bars and/or Law Societies from the respective Member States entirely satisfy the requirement of complete independence postulated by the Court.

c) Clarify the rules applicable to lawyers, acting as data protection officers

The Commission envisages making the appointment of an independent Data Protection Officer mandatory and to harmonize the rules related to their tasks and competences.

In this respect, it will be necessary to clarify the rules applicable to lawyers, acting as data protection officers, in light of their professional secrecy obligations.

[1] Case C-518/07 of 9 March 2010, *European Commission v Federal Republic of Germany*, recital 50.

CCBE wishes to refer to the already existing national rules relating to lawyers acting as data protection officers, enabling lawyers to fulfil their role as data protection officers whilst maintaining their professional secrecy obligations. CCBE refers for example to the French article 6.2.2 on the activity of data protection officer in the French *Règlement Intérieur National de la Profession d'avocat.*[2]

d) Participation of CCBE to WP29 activities

The European Commission states in its Communication that the Article 29 Working Party should become a more transparent body.

Taking into account the enormous impact of this Working Party on the interpretation and practical application of the data protection legal framework within the European Union and beyond, the CCBE fully shares the view of the Commission that the Working Party should become more transparent in its procedures and working methods.

As the legal profession is regarded as a fully independent profession with very specific requirements when it comes to data protection compliance, the CCBE believes the activities of the Working Party should be opened to representatives of the legal profession.

e) Redefinition of judiciary data as sensitive data

In relation to the processing of sensitive data, a category which needs to be further considered is personal data used in civil or criminal procedures, also called judiciary data. At present, judiciary data is not explicitly mentioned as a special category of data within the scope of Article 8 of the Data Protection Directive. The current directive merely provides that the processing of personal data used in civil or criminal procedures, "may be carried out only under the control of official authority, or if suitable specific safeguards are provided under national law, subject to derogations which may be granted by the Member State under national provisions providing suitable specific safeguards."

The CCBE calls upon the European Institutions to seek to harmonise rules for minimum protection of personal data in judicial proceedings, but always respecting the existing rules and practices in member state jurisdictions with regard to the public nature of judicial proceedings.

f) Fewer administrative formalities

The current system of notifications for notifying data processing activities imposes an unnecessary burden on the data controller, especially the lawyer working as a sole practitioner.

The CCBE supports the suggestion of the European Commission to lower the administrative burden for businesses and organisations whilst ensuring effective data protection.

g) Extraterritorial issues: engage in negotiating binding international agreements with non-EU states

No matter how effective a revised EU data protection regime may be, it will be ineffective where the activity which it sought to regulate is carried out by entities outside the territorial jurisdiction.

The CCBE is of the opinion that the European expertise in data protection rules and technical solutions should be promoted on an international level, especially since new information and communication technologies (e.g. cloud computing) may lead to personal data being stored outside of the European Union without the controller nor the data subject being aware of the location.

---

[2] Article 6.2.2 du Règlement Intérieur National de la profession d'avocat (RIN) : l'activité de correspondant à la protection des données personnelles (L. n° 78-17 du 6 janv. 1978, art. 22 ; D. n° 2005-1309 du 20 oct. 2005, art. 49 et s.)
6.2.2.1 Dans son activité de correspondant à la protection des données personnelles, l'avocat reste tenu de respecter les principes essentiels et les règles du conflit d'intérêt.
6.2.2.2 L'avocat correspondant à la protection des données personnelles doit mettre un terme à sa mission s'il estime ne pas pouvoir l'exercer, après avoir préalablement informé et effectué les démarches nécessaires auprès de la personne responsable des traitements ; en aucun cas il ne peut dénoncer son client.

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. The essential elements that need to be considered when negotiating such 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 to have recourse to the courts to seek legal remedies).
- That an independent monitoring body is provided for.

h) Codes of Practice and self-regulation

The European Commission plans to explore the possible creation of EU certification schemes (e.g. 'privacy seals') for 'privacy-compliant' processes, technologies, products and services.

Though supportive of Codes of Practice and self-regulation, the CCBE warns against falling into an overzealous assumption that additional schemes of certification or registration would necessarily be desirable.

In each case it should be asked, what, if anything, could be achieved beyond what is already capable of being achieved by Codes of Practice and self-regulatory or voluntary schemes. It may be that suggestions that there should be some form of certification or registration with a 'seal' would be both bureaucratic and unnecessary, and serve only to increase the cost of doing business.

Bearing this in mind, the use of certification schemes for data protection, which are applicable to those responsible for data processing, is an approach that deserves our attention. It is ultimately easier to control whether a procedure and specifications have been met rather than determining whether the prohibitions imposed by law have been violated. Obtaining such seals of approval which acknowledge that the person responsible for the file has fulfilled his/her obligations, has the following advantages:

- Proactive and voluntary approach
- Well-defined and fully audited data protection procedures
- Problems are solved first with further checks being scheduled- Better image for the company which has the seal of approval.

However, a purely coercive control has the following disadvantages:

- Operations are imposed and reactive.
- Domain is limited and often only partially audited
- Identified problems are solved later

In this perspective and to avoid the multiplication of labels (with inevitably mixed minimum requirements), increasing number of national procedures and additional costs, it would be useful to establish a European system of certification.

i) Data protection rules in the area of police and judicial cooperation in criminal matters

The Data Protection Directive applies to all personal data processing activities in Member States in both the public and the private sectors. However, it does not apply to the processing of personal data 'in the course of an activity which falls outside the scope of Community law', such as activities in the areas of police and judicial cooperation in criminal matters**.**

The CCBE agrees with the analysis from the European Commission stated in its Communication[3] and therefore supports the extension of the application of the general data protection rules to the areas of police and judicial cooperation in criminal matters, including for processing at domestic level while

[3] See COM(2010) 609 final, Chapter 2.3, p. 13-14.

providing, where necessary, for harmonised limitations to certain data protection rights of individuals, e.g., concerning the right of access or to the principle of transparency. However, such an extension, in any case must take into account the peculiarities of the work of lawyers and the prevalence of right to counsel and effective legal protection.

3. CCBE Recommendations

The CCBE therefore urges the European institutions to take into account the following guidelines when shaping Europe's legal framework on the fundamental right to protection of personal data:

1. 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;
2. to ensure that lawyers' professional secrecy prevails over all data protection rules;
3. to ensure that the supervision of compliance with data protection rules by lawyers shall be exclusively accomplished by a special independent authority that is familiar with the interests of the legal profession;
4. to clarify the rules applicable to lawyers, acting as data protection officers, in light of their professional secrecy obligations;
5. to open the activities of the Working Party 29 to representatives of the legal profession;
6. to seek to harmonise rules for minimum protection of personal data in judicial proceedings, but always respecting the existing rules and practices in member state jurisdictions with regard to the public nature of judicial proceedings;
7. to lower the administrative burden related to the current notification system for data controllers;
8. to engage in negotiating binding international agreements with non-EU states so as to increase internationally the extent of the protection of personal data;
9. to take a realistic/pragmatic approach towards privacy certification schemes;
10. to extend the application of the general data protection rules to the areas of police and judicial cooperation in criminal matters providing, where necessary, for harmonised limitations to certain data protection rights of individuals, and taking into account the peculiarities of the work of lawyers and the prevalence of right to counsel and effective legal protection.

Furthermore, the CCBE wishes to reiterate once again the following guidelines stemming from its earlier position[4] to a review of the data protection legal framework:

1. to ensure that lawyers' professional secrecy is guaranteed in the context of data protection when retained traffic and communication data are accessed by governments and other competent authorities;
2. to ensure that access to retained data is granted under the legislation only with prior judicial authorisation;
3. to ensure that once the government or law enforcement authority has accessed the data, it should only be used and stored for as long as this is necessary for the purpose for which the data was originally supplied as protected under Article 6 of the Directive 95/46/EC and Article 6 Para 1 of the Directive 2002/58/EC;
4. to ensure that a high level of protection measures safeguarding the principle of respect for privacy and confidentiality of communications, as protected under Articles 7 and 8 of the Charter of Fundamental Rights of the European Union and Article 8 of the European Convention of Human Rights, are inserted into the legislation.

[4] CCBE position on the Legal Framework for the Fundamental Right to Protection to Personal Data

Finally, the CCBE would like to express its willingness to provide further input and expertise to future consultations or proposals from the European Commission in this field.