International Chamber of Commerce
The world business organization

PEACE AND PROSPERITY THROUGH WORLD TRADE
90 YEARS
1919-2009
INTERNATIONAL CHAMBER OF COMMERCE

Prepared by ICC Commission on

E-Business, IT and Telecoms

ICC Response to the European Commission Consultation on the Legal Framework for the Fundamental Right to Protection of Personal Data

(December 2009)

ICC Response to the European Commission Consultation on the Legal Framework for the Fundamental Right to Protection of Personal Data

(December 2009)

ICC is pleased that the European Commission has invited public comment on the legal framework for the fundamental right to data protection in the EU.[1] ICC's comments are directed towards the EU Data Protection Directive 95/46/EC as the basic legal instrument governing the right to data protection in the EU.

ICC has been actively involved for many years in constructive dialogue with the Commission and other international bodies (such as APEC and the Council of Europe) regarding data protection. ICC's efforts have resulted in the drafting of instruments to facilitate data protection and international data flows, such as the alternative controller-to-controller standard contractual clauses originally approved by ICC and approved by the Commission (2004); the standard application form for binding corporate rules (BCRs) approved by the Article 29 Working Party (2006); and the new set of controller-to-processor standard contractual clauses currently being considered by the Commission.

The Directive was finalized prior to the vast expansion of Internet access and use of sophisticated electronic communications. This consultation provides an opportunity for the Commission to evaluate whether changes are necessary to the Directive to accommodate the Internet, mobile commerce, and other innovations in the information economy to reflect current business realities.

General comments

ICC and its thousands of members strongly support the protection of personal data, which has proven to be a critical factor to enable consumer confidence and online commerce. ICC also believes that the fundamental data processing principles upon which the Directive is based (such as legitimacy, purpose limitation, transparency, proportionality, security, and control) have proven themselves over the years, and do not need to be changed. However, ICC is also of the opinion that certain provisions of the Directive do give rise to problems and need to be re-thought.

ICC would also like to point out that there are significant problems relating to implementation of the Directive in the Member States. We realize that a detailed review of implementation of the Directive exceeds the scope of this consultation. However, more work should be done to ensure that Member States do not implement the Directive in a way that exceeds its core obligations so as not to undermine the internal market. We have included herein several examples of problems with implementation of the Directive.

[1] *See* http://ec.europa.eu/justice_home/news/consulting_public/news_consulting_0003_en.htm

Specific comments

ICC would like to direct the Commission's attention to the following specific issues. In each case, a short description of the problem is followed by a suggestion for further action. ICC strongly believes that action on the following points is necessary if the Directive is to retain its relevance in light of new technologies and the growing globalization of data processing.

- Recitals: A recital should be added mentioning the fact that the right to data protection is to be balanced against other fundamental rights and legal obligations (as set forth in the 2008 ECJ *Promusicae* judgment).

- Applicable law and jurisdiction: There are a number of issues which require the Commission's attention with regard to Article 4 of the Directive (dealing with applicable law and jurisdiction):
  - *Uncertainty as to which law applies to data processing*: There are many situations where it is difficult to determine which Member State data protection law applies to data processing, or whether EU data protection law applies at all. This can arise in cases such as outsourcing of a non-EU activity to an EU-based service provider, or localization of a database in Europe processing data collected by entities around the world and then re-exporting the data to third countries. Some national DPAs (for example, in Germany) have published their own interpretations of applicable law issues, but seemingly without coordinating them with the Commission or the Article 29 Working Party, which can lead to conflicts when different DPAs take differing views of whether EU data protection law applies.
  - *Conflicts between data protection law and other laws*: There are an increasing number of cases where conflicts arise between data protection law and other fundamental rights and legal requirements (e.g. e-discovery, whistle blowing etc.), which puts businesses in the position of not knowing which law to comply with.
  - *Jurisdiction based on the use of "equipment" in the EU (Article 4(1)(c) of the Directive)*: Deeming non-EU data controllers to be "using" equipment in the EU when an EU individual goes to their web sites using various automated tools (such as cookies) is a legal fiction that implies that the vast majority of foreign websites is subject to EU data protection rules, since most websites make use of such tools. Furthermore, this also means that a foreign website operator would become subject to the laws of all Member States, since the applicable law would depend on the then current location of the visitor of the website. The criterion of "use of equipment" as contained in Article 4(1)(c) of the Directive seems both too tenuous and unclear to serve as a sufficient jurisdictional link.

  Suggestions:
  - The Commission should convene a group of experts on data protection and private international law to examine the proper legal rules for applicable law and jurisdiction in the Directive. Ideally such rules would be

based on other Community legal instruments, such as the Brussels Regulation, to ensure a coordinated approach to these questions. The Commission should then adopt a communication with concrete examples explaining when EU data protection law applies and when it does not.
- DPAs should be asked to notify their own interpretations of applicable law and jurisdictional criteria to the Commission and their colleagues in the Article 29 Working Party before adopting them.
- Article 4(1)(c) of the Directive should be revised to base jurisdiction on grounds other than the "use of equipment"; examples of such grounds could be the level of control that a data controller has over data processing, and the level of transparency that is provided concerning data collection.

- Clarification of basic data protection concepts: There is a lack of clarity and harmonization regarding the definition of a number of basic data protection concepts contained in Article 2 of the Directive (such as "data controller", "data processor", "co-controller", and "personal data"). This creates substantial uncertainty for both data controllers and data subjects. For example, the relationship between the concepts of data controller and data processor does not adequately cover all the entities involved in the processing of data, which is a result of the trends towards offshoring and outsourcing. This can result (for example) in companies having to conclude contractual clauses with each and every subcontractor they use, which is a competitive disadvantage for companies located in the EU.

  Suggestions:
  - The distinction between "data controller" and "data processor" should be abolished, and each party that processes personal data should be responsible and liable based on its own role in the data processing. The Workshop on the Distinction between Data Controllers and Data Processors held at ICC headquarters in Paris on 25 October 2007[2] demonstrated that the distinction between the two terms no longer makes sense given the reality of global data flows. Existing concepts of agency law and tort law already provide a sufficient legal framework for assessing the responsibility of parties involved in data processing, without forcing them into a limited set of categories that does not fit reality.
  - When defining "personal data", account should be taken of whether the data processor or controller has a realistic possibility of linking data to a given individual, considering its practical ability to actually identify the individual, the time and manpower that would be required, and the purpose of identifying the individual in the framework of the organization's activities. There are many situations where there is no need to consider data processed in such circumstances to be "personal data".

[2] *See the report on the meeting at* http://www.iccwbo.org/policy/ebitt/id17896/index.html?terms=%22data+controller%22

- Cooperation with the private sector and action to ensure a more pan-European view of data protection: Since the first evaluation of the Directive in 2003, the Commission has devoted most of its attention to issues relating to law enforcement and data protection (e.g., PNR data, access to SWIFT data, etc.), and not enough attention to those affecting the private sector (e.g., greater harmonization of data protection law, international data transfers, conflicts between EU data protection law and laws in third countries, and many others). Instead, private sector issues have been left to the Member States, with a result that the lack of harmonization of data protection law in practice has only increased:
    - *Lack of interest by the Commission in implementation of its own decisions*: In 2006 and 2007, ICC submitted to the Commission detailed information on problems in Germany and other Member States with implementation of Commission decisions regarding the standard contractual clauses. At that time, the Commission indicated to ICC that for political reasons, it was not able to follow up with DPAs on these issues.
    - *Lack of resources by the Commission to deal with private sector issues*: The Commission has taken action to encourage or even force certain Member States to ensure the independence of their DPAs, and to see that DPAs have sufficient resources to do their jobs. However, it seems that the Commission itself has insufficient personnel dealing with data protection issues as they affect the private sector.
    - *Lack of guidance by the Commission on issues of pan-European importance*: As guardian of the Treaties, the Commission should actively promote a more pan-European view of crucial data protection concepts, and also take action to see that Member States respect Commission decisions, which action has been conspicuously lacking since first evaluation of the Directive. This is one of the reasons that there has been little interest by the private sector in approval of pan-European Codes of Conduct under Chapter V of the Directive, since use of such Codes is of little use if they are interpreted differently in different Member States. The need for guidance from the Commission is also crucial in light of recent changes to the e-Privacy Directive 2002/58, which may lead Member States to adopt different approaches to issues that require a harmonized approach (such as security breach notification).
    - *Lack of impact assessment of data protection initiatives:* It seems that many data protection initiatives are begun by the Commission and the Article 29 Working Party without adequately considering their economic impact.
    - *Role of the Article 29 Working Party:* While the Working Party has become more transparent in recent years, there is still a need for greater transparency.

  Suggestions:
    - The Commission should take a more active and aggressive stance to ensure that Member States and DPAs properly implement Commission decisions in the area of data protection, and do not frustrate them through

the imposition of national requirements. In this regard, the Commission should issue a communication (based on specific examples and information, which ICC would be happy to provide) to clarify the boundaries beyond which Member States may not go in implementing Commission decisions.

- The Commission should issue interpretative communications on questions raised by the data protection directives that are of European importance. As an example, the recent introduction into the e-Privacy Directive 2002/58 of a security breach notification requirement raises many questions of interpretation that may be implemented differently in different Member States, which lack of harmony would put substantial burdens not only on data controllers, but also on DPAs. Such pan-European guidance from the Commission is particularly important since it seems likely that the breach notification requirement will gradually be extended to all types of data controllers and processors (i.e., beyond telecom service providers and ISPs as is now the case).
- The Commission should be provided with increased personnel and resources so that it can deal with private sector data protection issues adequately.
- The Article 29 Working Party should increase transparency in its work. This could include, for example, the following steps: engaging in more consultations with private sector representatives; making more consultations open to the public (which could include webcasting them); and publishing on its web site details of such consultations.
- Each data protection initiative of the Commission and the Working Party should contain a discussion of its economic implications.

- International data transfers: Significant problems exist with regard to the regulation of international data transfers under Chapter IV of the Directive, in particular the following:
  - The issuance of "adequacy" decisions by the Commission under Article 25 of the Directive does not function properly and requires urgent attention. Only a handful of such decisions have been issued by the Commission in the 10 years since the Directive came into force, which demonstrates the scope of the problem. Political factors sometimes enter into the process of negotiating adequacy determinations, and in effect the standard that must be met seems to be "equivalency" with EU law, rather than "adequacy" as is required by the Directive.
  - As discussed further above, Commission decisions regarding international data transfers (such as adequacy decisions, and decisions concerning the standard contractual clauses) are not implemented in a harmonized manner. Member States and DPAs are allowed to interpret the decisions in a piecemeal fashion, with little or no control by the Commission. The following are just a few examples of such differences in implementation in the Member States with regard to use of the standard contractual clauses (ICC has already submitted this information, as well as further examples, to the Commission in 2007):

- Austria: The DPA requires that the annexes to the standard contractual clauses be drafted in a very detailed manner and that all elements of the data that are to be transferred be listed in detail in Annex B. This goes beyond what is required in the clauses, where the annexes only require the listing of "categories of data". In addition, applicants must enter into a new set of clauses and obtain additional DPA approval each time a single new item of data is to be transferred.
- The Netherlands: The DPA routinely requests detailed information on how the personal data are protected in the case of onward transfers to third party data processors by a non-EU data controller. In particular, the DPA requests information about how transfers to third parties are safeguarded and in which way these third parties will be bound by the standard contractual clauses.
- Poland: The DPA routinely rejects the use of standard contractual clauses for certain types of data transfers (e.g., for whistleblower hotlines), and instead requires that the data controller in the US to whom the data are be transferred join the Safe Harbor.
- Slovenia: The DPA requires that separate applications be filed for each country to which the data are to be transferred. Thus, if the data are to be transferred to thirty corporate subsidiaries around the world, it is necessary to file thirty applications. The DPA also requests copies of the commercial register extracts of the data importers to prove that they are actually members of the data exporter's corporate group. Obtaining these commercial register extracts from many countries can take months and make use of the clauses practically impossible.

- While substantial improvements have been made recently to the mutual recognition system for approval of BCRs, the procedure still takes too long and is subject to too many inconsistent requirements. For example, every time a new improvement to the BCRs approval system is announced, some DPAs require companies that have nearly completed the process to start over and obtain further approvals taking the new requirements into account. There is also a lack of transparency about what national requirements exist with regard to approval of BCRs.
- ICC appreciates the work the Commission has done toward approval of the alternative controller-to-processor standard contractual clauses which ICC and other business groups have proposed. However, the reality of transfers to data processors in today's business world means that the use of standard contractual clauses (which is often the only practical way to ensure "adequacy" under the present system) is not sufficient, and different ways need to be explored to provide a legal basis for transfers to data processors.

<u>Suggestions</u>:

- If the present system of adequacy is retained, it requires a radical overhaul, which should include the following steps: 1) more financial and personnel resources in the Commission and the DPAs should be devoted

to adequacy decisions and other international data transfer issues; 2) the Commission should adopt tools and "best practices" for adequacy decisions (such as preparation of standardized checklists that countries would use in preparing for an adequacy review, and setting standardized deadlines for the various steps in an adequacy determination); 3) greater transparency should be created for adequacy determinations (such as by regular information of the public about countries that have applied for adequacy, and the status of such applications); and 4) making greater use of adequacy decisions covering a specific industry, a specific type of data processing, or a specific law or regulation, which should be quicker and easier to reach than those covering entire countries, and could be fine-tuned to cover types of data transfers and data processing where there is the greatest need for adequacy decisions. All of these measures would help streamline the adequacy process.

- Greater attention should be paid to whether individual parties transferring personal data provide "accountability" for data processing. Accountability has several important advantages over adequacy, such as: 1) it does not require the enactment of decisions covering an entire country or sector in a lengthy and cumbersome process, but is determined based on the precautions taken by a particular data exporter; 2) it ensures that there is always a party in the individual's own country who remains liable and to whom the individual may turn if there is a problem with regard to the processing of the personal data outside of the EU; and 3) it avoids quixotic attempts to convince third countries to conform their law to EU standards, which process tends to lead to tensions with such countries. In this regard, use should be made of the experience of countries that already have an accountability system in place (such as Canada), and of work presently being carried out on accountability by the OECD.
- The Commission should take a more active and aggressive stance to ensure that Member States and DPAs properly implement Commission decisions in the area of international data transfers, and do not frustrate them by making them subject to national requirements. In this regard, the Commission should issue a communication to clarify the boundaries beyond which Member States may not go in implementing Commission decisions (these points are also made above). An inventory of national requirements should also be published to increase transparency.
- The existing mutual recognition system for approval of BCRs should be enhanced so that approvals are more streamlined and not as subject to individual DPA requirements. In this regard, Article 26 of the Directive should be amended to give the Commission the ability to approve BCRs on a pan-European basis. The Commission and the Article 29 Working Party should also publish a definitive list of what national requirements exist regarding approval of BCRs. In addition, the Commission and the Article 29 Working Party should explore the use of BCRs for transfers to outside data processors.

- Notification of data processing: Notification of data processing under Section IX of the Directive remains an area which requires attention. The Commission's "First Report on the implementation of the Data Protection Directive (95/46/EC)"[3] issued in 2003 describes the differences in the notification requirements in Member States as "a matter of concern" (p. 12), and the situation has hardly improved since then. In fact, there is virtually no harmonization at all among the Member States in the area of notifications to DPAs, so that a single database that may be accessed in multiple Member States must be potentially notified in 27 different ways . It is not even clear what purpose notification requirements serve: they are hardly ever consulted by individuals, and some DPAs have indicated privately to ICC that they view notifications as a burden and that they hardly have the resources to make use of the information that is provided by them.

  Suggestions:
  - The Commission and the Article 29 Working Party should develop a template for a pan-European notification form, and then invite DPAs to modify their national forms and procedures to match it as closely as possible.
  - The Commission should investigate the creation of a single pan-European notification that would apply in all Member States. This could involve the creation of a "data protection passport" that would make multiple notifications unnecessary. If necessary this could involve amendment of the Directive.
  - In some Member States certain types of routine data processing are either exempt from notification, or are subject to a simplified notification regime, which is of particular benefit to small and medium-sized enterprises (SMEs). The Directive could be amended along these lines.
  - Since it seems that some DPAs rely on notifications as a method to raise revenue and fund their operations, the Commission should insist that Member States properly fund DPAs so that they are not forced to resort to notifications as a fund-raising measure.
  - The role of the company data protection officer (DPO) should be strengthened, if necessary by amendment of the Directive. In particular, making data controllers exempted from the duty of notification if they appoint a data protection officer.

*** *** ***

[3] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2003:0265:FIN:EN:PDF

The International Chamber of Commerce (ICC)

The International Chamber of Commerce is the largest, most representative business organization in the world. Its hundreds of thousands of member companies in over 130 countries have interests spanning every sector of private enterprise.

A world network of national committees keeps the ICC International Secretariat in Paris informed about national and regional business priorities. More than 2,000 experts drawn from ICC's member companies feed their knowledge and experience into crafting the ICC stance on specific business issues.

The United Nations, the World Trade Organization, and many other intergovernmental bodies, both international and regional, are kept in touch with the views of international business through ICC.

For more information please visit: www.iccwbo.org

ICC Commission on E-Business, IT and Telecoms (EBITT)

Business leaders and experts drawn from the ICC membership establish the key business positions, policies and practices on e-business, information technologies and telecommunications through the EBITT Commission. With members who are users and providers of information technology and electronic services from both developed and developing countries, ICC provides the ideal platform to develop global voluntary rules and best practices for these areas. Dedicated to the expansion of cross-border trade, ICC champions liberalization of telecoms and development of infrastructures that support global online trade. ICC has also led and coordinated the input of business around the world to the World Summit on the Information Society, Geneva 2003, Tunis 2005, and continues this effort in the activities established in the Tunis Agenda through its initiative, Business Action to Support the Information Society (BASIS http://www.iccwbo.org/basis)

International Chamber of Commerce
The world business organization
Policy and Business Practices
38 Cours Albert 1er, 75008 Paris, France
Tel +33 (0)1 49 53 28 28 Fax +33 (0)1 49 53 28 59
E-mail icc@iccwbo.org Website www.iccwbo.org