5092/98/EN/final
WP 15

Working Party on the Protection of Individuals with regard to the Processing of Personal Data

OPINION 1/99

concerning
the level of data protection in the United States and the ongoing discussions between the European Commission and the United States Government

Adopted by the Working Party on 26 January 1999

Opinion concerning
the level of data protection in the United States and the ongoing discussions between the European Commission and the United States Government

The Working Party is aware of the ongoing discussions between the European Commission and the United States Government which are seeking to guarantee both high levels of protection for personal data and the free movement of personal information across the Atlantic. The Working Party attaches importance to these discussions and hopes that it will prove possible to reach a positive outcome as soon as possible. In the light of this discussion, a letter and its annex signed by M. Aaron on 4 November 1998 has been transmitted which contains a certain number of proposals intended to be discussed inside the USA by representatives of US companies with the Federal Department of Commerce. In this context the Working Party urges the parties to these discussions and the EU Member State governments meeting in the committee established by Article 31 of Directive 95/46/EC[1] to take into account the following points.

Data protection rules are not only intended to protect users of new technologies (in particular informatics and Internet) with a view to guaranteeing trust and confidence and thus to provide for the development of these technologies and the exchange of data at international level. These rules express also the adherence to a certain number of fundamental principles and rights based on a common culture of respect for privacy and other values that are inherent in the human being and which is shared equally by the Member States of the European Union and the United States.

1. Privacy and data protection in the United States is found in a complex fabric of sectoral regulation, at both federal and state level, combined with industry self-regulation. Considerable efforts have been made during recent months to improve the credibility and enforceability of industry self-regulation, particularly in the context of the Internet and electronic commerce. Nevertheless, the Working Party takes the view that the current patchwork of narrowly-focussed sectoral laws and voluntary self-regulation cannot at present be relied upon to provide adequate protection in all cases for personal data transferred from the European Union.

2. Given the complexity of the US system of privacy and data protection, the establishment in the US of an agreed "benchmark" standard of protection in the form of a set of "safe harbor" principles offered to all economic actors and US operators is a useful approach which might need to be complemented by contractual solutions in certain specific cases. However, further improvements are needed if free movement of data to the United States is to be ensured on the basis of these privacy principles. In addition, it might be necessary to provide for a methodology which makes clear which companies are covered by the “safe harbor” principles.

3. It has to be noted that the decision to adhere to the set of principles belongs solely to the individual company, and so the problem of those companies which do not wish to apply the principles remains whilst no overall legislation exists.

[1] 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, JO L 281, 23 November 1995, p. 31. Available at http://www.europa.eu.int/comm/dg15/en/media/dataprot/index.htm.

4. Generally, the status of these principles needs to be clarified. Whilst adherence to the principles in the first instance can be voluntary, once a company does decide to adhere and thereby to claim the benefit of “safe harbor”, compliance must be compulsory.

5. The credibility of the system is seriously weakened by the lack of a requirement for independent compliance monitoring and by relying solely on company self-certification. Independent verification would need to be serious but could at the same time be practicable, even for small companies. Models currently being developed in the US by the Better Business Bureau OnLine and Trust-E are going in the right direction.

6. It must be possible for complaints from individuals whose data have been transferred from the EU to be dealt with in a practical and effective manner, and adjudicated upon, in the final instance, by an independent body. A key issue in this regard is the identification of one or more independent public bodies or third party organisations in the US that are willing and able to act as contact points for EU data protection authorities and to co-operate in the investigation of complaints. Care must be taken to ensure that practical arrangements are in place for all relevant US sectors. Existing regulatory agencies, such as the Federal Trade Commission and the Office of the Comptroller of the Currency can perform such a role in the areas for which they have competence.

7. In terms of its substantive content, any acceptable set of "safe harbor" principles must, as a minimum requirement, include all the principles set out in the OECD Privacy Guidelines of 1980, adopted amongst others by the United States and recently re-endorsed at the OECD's Ottawa Conference on Electronic Commerce. These principles are also applied by Directive 95/46/EC as well as by national legislation of the Member States of the European Union. In this regard, the above mentioned consultative text of principles published by the US Department of Commerce on 4 November 1998 raises some concerns, in particular:

    a) The individual's right of access is limited to that which is "reasonable". The OECD Privacy Guidelines do not limit the right itself, simply asserting that it must be exercised "in a reasonable manner".

    b) The purpose specification principle of the OECD Privacy Guidelines is absent, and is only partly replaced by a "choice" principle which in effect allows data collected for one purpose to be used for another, provided individuals have the possibility of opting out.

    c) Proprietary data and any manually processed data are entirely outside of the scope of the US principles, while the "choice" principle provides no protection to data collected from third parties and the "access" principle excludes public record-derived information.

    d) According to the third paragraph of the introduction, “adherence to the principles is subject to” a number of exceptions and limitations such as “risk

management" and "information security". The Working Party takes the view that these notions are too vague and open-ended, and recommends that they be clarified or deleted.

Done at Brussels, 26 January 1999

For the Working Party

The Vice-Chairman

Prof. Stefano RODOTA