Data Protection and the US: results of the meeting with EU-Member States, 26 October 1998

DN: BIO/98/477 Date: 1998-10-27

TXT: EN
PDF: EN
Word Processed: EN

bio/98/477

Bruxelles, le 27 octobre 1998

NOTE BIO AUX BUREAUX NATIONAUX

cc. aux Membres du Service du Porte-Parole

Data Protection and the US: results of the meeting with EU-Member States, 26 October 1998

(Betty Olivi)

After consulting the Member States, the Commission welcomed the broad support and encouragement it had received to continue its dialogue with the US on the application of the Data Protection Directive to transfers of personal data from the EU to the US and bring it to an operational outcome.

The Commission said it would continue its efforts to reach an understanding with the US designed to allow transfers of data to be made freely to US companies that sign up to a set of privacy principles to be issued by the US Department of Commerce.

The understanding promises to provide a predictable, workable framework for companies on both sides of the Atlantic in which the protection of EU citizens' data will be secured and the disruption of trans-Atlantic data flows avoided.

Discussions with the US will be held over the coming month or so, with a view to finalising the arrangements for the so-called "safe harbour". The Commission said it would like to see the current discussions with the US brought to a successful conclusion by the end of the year.

The Commission will keep the Member States involved in its talks with the US and in parallel discuss with the Member States the procedures through which the results of its discussions might be formalised on the EU side.

In the meantime, the Member States recognised the importance of avoiding the disruption of data flows to the US and indeed to other third countries engaged in good faith efforts to provide adequate protection for personal data.

Amitiés

Martine Reicherts

Impact of Directive 95/46/EC on transfers of Personal Data to non-EU countries

Background Briefing Not attributable

Directive 95/46/EC concerns the protection of individuals with regard to the processing of personal data within the EU and the free movement of such data. The Directive entered into effect on 25 October 1998 (see IP/98/925). Some of its provisions concern the conditions under which personal data can be transferred to countries outside the EU.

The application of these provisions has aroused interest and some concern among governments and economic operators outside the EU and led to discussions between the Commission's services and government representatives from the United States and other countries outside the Union. This note aims to provide background information on this issue and answers to some frequently asked questions.

The text of the Directive, a summary of its provisions and more background material are available at: http://europa.eu.int/comm/dg15/index.htm

1. What is the purpose of the Directive? Who will benefit from it?

At a time when an increasing quantity of personal data is processed and made available, the Directive spells out the basic individual rights to privacy: for example, every person should have the right of access to personally identifiable data relating to him/her, and a right to rectification of those data where they are shown to be inaccurate. In certain situations, he/she should also be able to object to the processing of his/her personal data. In addition, individuals should be provided with information as to the purpose of processing and the identity of the data controller, so that they can exercise their right of access. Where "sensitive" data are involved (for instance, medical data, and data revealing racial or ethnic origin, religious or philosophical beliefs), additional safeguards should be in place, such as a requirement that the person concerned gives his/her consent for the processing.

At the same time, the Directive ensures that companies and other organisations will be able to transfer personal data throughout the European Union. In most European countries, the protection of personal data is a constitutional principle, and the right to privacy is enshrined in the European Convention on Human Rights. Without the Directive, different national approaches to data protection would create barriers within the market and the free movement of personal information would be impaired. In harmonising data protection laws, the Directive ensures the free movement of personal data within the EU. The *raison d ' être* of the Directive is thus the Single Market.

2. When and where will these principles apply?

By 25 October 1998, the Directive was due to be implemented into national law by all fifteen Member States. Irrespective of the national implementation measures, certain provisions of the Directive will have direct effect in accordance with the case law of the European Court of Justice. The Directive will apply throughout the European Union, irrespective of whether the individuals concerned by the processing are EU citizens or not.

3. Why does the Directive deal with the transfer of data to non-EU countries?

The Directive establishes rules designed to ensure that data is only transferred to countries outside the EU when its continued protection is guaranteed or when certain specific exemptions apply (see questions 5 and 6 below). Without such rules, the high standards of data protection established by the Directive would quickly be undermined, given the ease with which data can be moved around on international networks.

The Directive provides for the blocking of specific transfers where necessary, but this is a solution of last resort and there are several other ways of ensuring that data continues to be adequately protected while not causing disruption to international data flows and the commercial transactions with which they are often associated.

4. How will this work?

The Directive requires Member States to permit transfers of personal data only to countries outside the

EU where there is adequate protection for such data, unless one of a limited number of specific exemptions applies. Where this is not the case, Member States must inform the Commission, which will start a Community procedure to ensure that any Member State decision to block a particular transfer is either extended to the EU as a whole, or reversed. In this task, the Commission is assisted by a committee and a working party. The committee, set up by Article 31 of the Directive, is composed of Member State officials. Its particular task is to advise the Commission concerning decisions on transfers to third countries.

The working party, set up by Article 29, is composed of the data protection commissioners or independent supervisory authorities of all the Member States. Its remit is wider than that of the committee and it will in particular play an important role in helping the Commission to ensure the even application of the Directive's requirements across the EU. All the documents adopted by the Article 29 working party are available at http://europa.eu.int/comm/dg15/index.htm .

5. Do we face the prospect of a "blackout scenario "?

Claims of a possible "blackout" in data flows between Europe and the rest of the World bear no resemblance to reality.

On the one hand, Article 25.4 of the Directive foresees that decisions to block transfers are taken on specific individual cases, raised by a Member State. A decision to block a transfer would only apply to other transfers of the same type, not to all transfers to the country concerned. There is a general interest in keeping the scope of such decisions as narrow as possible.

On the other hand, even where it is found that there is not adequate protection, transfers may take place in circumstances specified in Article 26. This will be the case when, for example:
the individual has given his unambiguous consent to the transfer, or
the transfer is necessary for the performance of a contract with the individual concerned (e.g.: employment contracts) or the implementation of pre-contractual measures taken in response to his/her request (e.g.: application for a job), or
the transfer is necessary or legally required for the establishment, exercise or defence of legal claims, or
the transfer is necessary in order to protect the vital interests of the individual (e.g.: transfer of medical data concerning an individual hospitalised in a non-EU country).

Other exceptions are provided by the Directive and show that, even for data flows to those countries which do not ensure an adequate level of protection, there are a generous number of bridges and doors. For some of these doors, the key is held by the individual. However, another door remains open even where the above conditions are not met, and the keys of this door are held by industry itself (see question 6).

6. To be "on the safe side ", what could interested companies do?

Companies operating worldwide may wish to establish safeguards that make them less dependent on the good will of the legislators of a given country. Even in the best case scenario, a number of non-EU countries are likely to fall short of an "adequate" level of protection, and individuals may be reluctant to give their consent to the transfer to such countries of their personal data. The Directive pays due attention to this reality, and Article 26 (second paragraph) recognises that adequate safeguards may be provided by the company itself. This provision specifies that these safeguards may in particular result from appropriate contractual clauses.

Contractual provisions binding the receiver of the data are one of the ways of providing the safeguards which make a transfer possible where the legislative or self-regulatory provisions in a non-EU country cannot themselves ensure "adequate protection". Such contract clauses would have to contain the same elements as the Commission is are looking for when assessing adequacy (such as access for the data subject, right to rectification, information on purpose of processing, legal remedies if privacy rights breached). The Article 29 group has already adopted (in April 1998) a document giving guidance on the role of contracts generally (available at http://europa.eu.int./comm/dg15/index.htm)

The Commission encourages the use of contracts in such circumstances and is currently considering the "model clauses" submitted by the International Chamber of Commerce on 23 September 1998.

7. Will the Directive apply to transfers of data which take place in the course of direct contacts with individual consumers on the Internet?

It would be rather illogical and without legal justification to "exempt" such an important means of transfer as the Internet from the scope of the data protection Directive. The EU Member States' data protection commissioners, meeting in the Article 29 group, have taken the view that the Directive does apply. The approach applied in traditional commerce, namely that a business actively seeking customers in another country subjects itself to that country's laws would tend to support this approach. It might be argued that an individual transferring his own data has given his consent to such a transfer, one of the exemptions from Article 25 allowed by Article 26, provided that he is properly informed about the risks involved. Guidance on the application of the Directive to the Internet will be provided by the Article 29 group.

8. Will technological developments not take care of the problem?

So-called "technological solutions", such as the use of on-line mechanisms to inform consumers and obtain their consent to the processing of their data, can play a useful role. A weakness, however, of such solutions is that they tend to place the burden of protecting personal data almost entirely on the individual, and furthermore, in the absence of a regulatory framework, there is no guarantee that businesses will adopt them. Market forces are unlikely to be sufficient to lead to their generalised use.

9. Which countries have adequate protection?

The procedure foreseen in Article 25.6 of the Directive has not yet been put to use so there are currently no formal decisions on "adequacy". Dialogues between the European Commission and a number of the EU's important trading partners are designed *inter alia* to improve our knowledge and understanding of their systems. Clearly countries which properly apply the Council of Europe's Convention no. 108 or the OECD guidelines and have rules which prevent data from being transmitted without safeguards to jurisdictions where this is not the case are likely to achieve or come close to the required standard.

10. Are the Directive 's provisions on data transfers to third countries compatible with world trade rules?

Yes. There is a specific provision in the GATS (Article XIV) which recognises the protection of personal data as a legitimate reason for blocking information flows and the free movement of services. Any such action would of course have to respect the general principles of proportionality and non-discrimination.

11. By banning transfers, will the EU not risk inflicting economic damage on itself and limiting its capacity to play a full part in global electronic commerce?

The aim of the Directive is to promote the flow of information, not to impede it. Ensuring the free movement of personal data within the EU by minimising differences between national rules for their protection was the *raison d ' être* of the Directive. By setting a high standard, the Directive fosters consumer confidence and thus encourages the development of electronic commerce.

The Commission fully recognises the undesirability of interrupting international information flows, which is why we are involved in discussions with our major trading partners with the aim of ensuring that the conditions for these flows are met. However, ignoring what happens to data transferred to third countries would render ineffective the rules we apply in the EU and so bans on specific transfers cannot be ruled out. We are convinced that strong guarantees for privacy are a necessary condition if electronic commerce is to thrive, not an obstacle to its development.

12. Why is the EU trying to impose its system on other countries? Is this not a case of "extraterritoriality "?

There is no desire to "export" the EU system to other countries. There are clearly different ways of arriving at the same results, but we need to ensure that the personal data of EU citizens transferred

outside the EU is being processed with due respect for certain widely accepted principles, that citizens can enforce their rights and that they are entitled to redress if they suffer damage as a result of a breach of these principles. We are conscious of the need to avoid procedures for blocking data transfers which are exclusively unilateral. Non-EU countries concerned need to be informed and given the chance to express their views.