EUROPEAN COMMISSION
Internal Market DG

FUNCTIONING AND IMPACT OF THE INTERNAL MARKET. COORDINATION. DATA PROTECTION
Data protection

Brussels, November 2001

PROTECTION OF PERSONAL DATA: IMPACT OF DIRECTIVE 95/46/EC ON TRANSFERS TO THIRD COUNTRIES

The Data Protection Directives was due to be implemented by the Member States by 25 October 1998. Directive 95/46 established rules of general application. Directive 97/66 specifies and complements these rules for the processing of personal data in the telecommunications sector. One of the important provisions of the general Directive concerns the conditions under which personal data can be transferred to third countries. The application of this provision has aroused interest and some concern among third country governments and among economic operators and led to discussions between the Commission's services and government representatives from the United States, Canada, Australia Japan and other third countries. This paper is designed to provide background information on this issue and answers to some commonly occurring questions.

1. The Directive

The Directive harmonises Member States' data protection laws with a view to ensuring the free movement of personal data within the EU while ensuring that the privacy of individuals enjoys a high level of protection. The *raison d'être* of the Directive is thus the Single Market. 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.

It is a framework Directive establishing basic principles which are applicable to all types of personally identifiable data, by whatever means they are processed. It places obligations on those who collect, process or transfer personal data and accords rights to data subjects (see box below). The Member States were required to transpose its requirements into their national legislation by 25 0ctober 1998. At the time of writing there are still three Member States (France, Luxembourg and Ireland) that have not implemented the directive and the European Commission has initiated proceedings against them before the Court of Justice for failure to comply.

The Directive establishes rules designed to ensure that data is only transferred to third countries when its continued protection is guaranteed or when certain specific exemptions apply (see section 2 below). Without such rules, the high standards of data protection established by the Directive would quickly be undermined, given the

Rue de la Loi 200, B-1049 Bruxelles/Wetstraat 200, B-1049 Brussel - Belgium - Office: C100 6/112.
Telephone: direct line (+32-2)296.6417, switchboard 299.11.11. Fax: 299.68010.
Telex: COMEU B 21877. Telegraphic address: COMEUR Brussels.

Fabrizia Benini @ cec.eu.int

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 associated.

The Commission is assisted in implementing the Directive by a committee and a working group. 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 group, 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. The Article 29 group is also asked to advise on certain aspects of data transfers to third countries.

The main principles governing the processing of personal data

1) **the purpose limitation principle** - data should be processed for a specific purpose and subsequently used or further communicated only insofar as this is not incompatible with the purpose of the transfer.

2) **the data quality and proportionality principle -** data should be accurate and, where necessary, kept up to date. The data should be adequate, relevant and not excessive in relation to the purposes for which they are transferred or further processed.

3) **the transparency principle -** individuals should be provided with information as to the purpose of the processing and the identity of the data controller in the third country, and other information insofar as this is necessary to ensure fairness.

4) **the security principle -** technical and organisational security measures should be taken by the data controller that are appropriate to the risks presented by the processing. Any person acting under the authority of the data controller, including a processor, must not process data except on instructions from the controller.

5) **the rights of access, rectification and opposition -** the data subject should have a right to obtain a copy of all data relating to him/her that are processed, 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 the data relating to him/her.

6) **restrictions on onward transfers to other third countries - where data are transferred to a third country, the recipient of the transfer should only be permitted to** transfer the personal data onwards to a new destination if adequate levels of protection are in place.

7) **the support and help provided to individual data subjects in the exercise of their rights** – The individual must be able to enforce his/her rights rapidly and effectively, and without prohibitive cost. To do so there must be some sort of

mechanism allowing independent investigation and adjudication of complaints, and an effective remedy where data protection principles are shown to have been breached.

Examples of additional principles to be applied to specific types of processing are:

1) **sensitive data -** where 'sensitive' categories of data are involved, additional safeguards should be in place, such as a requirement that the data subject gives his/her explicit consent for the processing.

2) **direct marketing -** where data are processed for the purposes of direct marketing, the data subject should be able to 'opt-out' from having his/her data used for such purposes at any stage.

3) **automated individual decision -** where the purpose of the processing is the taking of an automated decision, the individual should have the right to know the logic involved in this decision, and other measures should be taken to safeguard the individual's legitimate interest.

2. *What does the Directive say about transfers to third countries?*

The texts of Articles 25 and 26 of the Directive are annexed to this paper. There follows, in question and answer form, some guidance about what these Articles say, how they are likely to be applied and when and how further decisions on their application will be taken.

a) *What is the effect of the data protection directive on flows of data from the EU to Third Countries*?

The Directive, which had to be transposed into national law by October 1998, requires Member States to permit transfers of personal data only to third countries where there is adequate protection for such data, unless one of a limited number of specific exemptions applies. Where this is not the case, the transfer must not be allowed. There is a mechanism to ensure that any Member State decision to block a particular transfer is either extended to the EU as a whole, or reversed.

b) *Do we face the prospect of generalised bans on transfers to third countries which do not have adequate protection?*

No. Article 25.4 of the Directive foresees decisions to block transfers being taken on specific cases, raised by a Member State. Even where it is found that there is not adequate protection, transfers may take place in circumstances specified in Article 26, for example with the consent of the individual(s) concerned, or when specific contractual undertakings are in place. 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.

c) *Who decides on "adequacy" and on what basis?*

Cases will normally originate within a Member State, which will be required to notify its intention to block a transfer to the Commission. The formal decision of whether to confirm or override the Member State opinion rests with the Commission, but the Commission will be advised by a committee representing the Member States (Article 31 committee). A specialist advisory group (Article 29 working group) composed of the EU data protection supervisory authorities is also involved. By encouraging Member States to notify cases at an early stage even before their own procedures have been exhausted and by expediting the procedures at Community level, it is hoped that final Community-wide decisions on specific cases can be taken quite rapidly, thus minimising uncertainty and unnecessary disruption to economic activity.

The Article 29 group has produced a series of papers regarding the issue of transfers of data to third countries which can be given to outside contacts. At present there is one document (available at www.europa.eu.int./comm/dg15/en/index), outlining core data protection principles to be taken into consideration when assessing adequacy, examining self-regulatory systems in third countries, and looking at contractual solutions to international data flows (WP 12). The paper underlines the importance of examining both the content of rules and the manner in which they are enforced, in any assessment of the adequacy of protection. The Commission uses this advice in evaluating a third country's level of protection for personal data.

d) What are the procedures for the adoption of an Article 25.6 Commission decision recognising a third country as providing for adequate protection?

The Council and the European Parliament have given the Commission the power to determine, on the basis of Article 25.6 of the directive, whether a third country ensures an adequate level of protection by reason of its domestic law or of the international commitments it has entered into.

The adoption of a (comitology) Commission decision based on Article 25.6 of the Directive involves:

- a proposal from the Commission,
- an opinion of the group of the national data protection commissioners (Article 29 working party)
- an opinion of the Article 31 Management committee delivered by a qualified majority of Member States.
- European Parliament right of scrutiny, for a thirty-day period to check if the Commission has used correctly its executing powers, before the Commission adopts its decision.

The formal process of considering whether a specific legislative act meets the "adequacy" requirement can only commence once the relevant legislation is passed. The effect of such a decision is that data can flow from the fifteen EU MS and three EEA member countries ((Norway, Liechtenstein and Iceland) to that third country without any further safeguard being necessary. The Commission has so far

recognised Switzerland, Hungary and the US Department of Commerce's Safe harbor as providing adequate protection[1].).

d) Can self-regulation provide adequate protection?

The EU thinks that a fundamental individual right like privacy is important enough to be protected by the law and this is the approach we prefer. With their rights and obligations enshrined in law, individuals are entitled to have their privacy respected as a general rule, not just when they opt for privacy on the basis of choices offered by a business selling them a good or a service; and the business knows it faces sanctions if it violates those rights, not just the individual customer's sanction of going to find another supplier.

However, in assessing the adequacy of protection in third countries, we are more concerned with the content and effectiveness of the measures in place than with their form. Self-regulatory systems are therefore not, by definition, inadequate. In the same way as for laws, self regulatory systems will be considered adequate if they cover the principles enumerated above, are effectively enforced and offer a means for the individual to exercise his rights and gain redress if necessary. The existence of a mechanism through which individual complaints can be properly investigated and the presence of a neutral arbiter to adjudicate in cases where it is alleged that the rules have been broken will be considered important parts of such a system.

e) 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.

f) Won't the case-by-case approach lead to much uncertainty among economic operators and others involved in the transfer of personal data across borders?

The Commission aims to keep uncertainty to a minimum. One way is provided for in Article 25.6 of the Directive which allows the Commission, after consulting the Article 31 committee, to determine that protection is adequate in a particular country. It may be useful, in the case of some countries where we cannot conclude that protection is adequate as a general rule, to determine that adequate protection is provided for in some sectors.

g) Which countries have adequate protection?

So far we have formally recognised Switzerland, Hungary and the US Safe harbor principles as providing for adequate protection. Our dialogues with a number of

---

[1] Commission decisions 2000/518/EC (Switzerland); 2000/519/EC (Hungary) and 2000/520/EC (US Safe harbor principles) in OJ L 215 of 25.8.2000. Available also on our website europa.eu.int/comm/privacy

important trading partners continue and 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.

It is currently in the process of recognising the Personal Information Protection and Electronic Documents Act as adequate for the purposes of transferring data from the EU to Canada (at the time of writing the draft commission decision is before the European Parliament and we expect its go ahead in the first week of December. We are also in the process of examining the Argentinean Habeas Data Law.

h) What is the role of contractual solutions?

Contractual provisions are one of the ways of providing the safeguards which make a transfer possible where the surrounding circumstances do not amount to "adequate protection". They would have to contain the same elements as we are looking for when assessing adequacy. In many cases, specific contractual clauses will be an expensive option and more generalised measures to secure "adequate protection" are preferable. Moreover, in some Member States, an individual whose data is being processed cannot normally acquire rights from a contract to which he is not party (the contract would normally be between, for example, two companies involved in processing the data). Nevertheless, many economic operators will need to rely on contractual arrangements for transfers to countries where protection is not adequate or if there is any uncertainty about the adequacy of protection in the country of destination. The Commission encourages the use of contracts in such circumstances (unless of course one of the other exemptions provided for in Article 26 applies and provides a simpler solution) and is ready to give guidance, with the assistance of the Article 29 group, by approving standard contractual clauses. The Article 29 group has already adopted (WP 12) a document giving guidance on the role of contracts generally (available at europa.eu.int/comm/privacy))

i) Will the Commission adopt standard contractual clauses

Yes. The Council and the European Parliament have given the Commission the power to decide, on the basis of Article 26 (4) of directive 95/46/EC that certain standard contractual clauses provide adequate safeguards with respect to the protection of the privacy and fundamental rights and freedoms of individuals and as regards the exercise of the corresponding rights. The procedure to be followed is the same as for an adequacy finding.

The effect of such a decision is that by incorporating the standard contractual clauses into a contract, personal data can flow from a Data Controller established in any of the fifteen EU MS and three EEA member countries (Norway, Liechtenstein and Iceland) to a Data Controller established in a country not ensuring an adequate level of data protection without any additional safeguards being necessary.

On 15 June 2001, the European Commission adopted a Decision[2] setting out standard contractual clauses ensuring adequate safeguards for personal data transferred from the EU to countries outside the Union. The Decision obliges Member States to recognise that companies or organisations using these standard clauses in contracts concerning personal data transfers to countries outside the EU are offering "adequate protection" to the data. The use of these standard contractual clauses is voluntary but it offers companies and organisations a straightforward means of complying with their obligation to ensure "adequate protection" for personal data transferred to countries outside the EU which have not been recognised by the Commission as providing adequate protection for such data.

The Commission is in the process of approving standard contractual clauses for transfers of personal data to data processors. The proposal has received the approval of the EU Data protection commissioners and the EU Member States meeting in the Management committee and is currently being forwarded to the European Parliament for the exercise of the right of scrutiny.

j) Are you intending to apply the Directive to transfers of data which take place in the course of direct contacts between individual consumers in the EU and businesses on the Internet?

Yes. The European data protection legislation applies to data collected and further processed using automated equipment located in the territory of the EU and the EEA There would be something illogical about – and there is no legal justification for - "exempting" such an important means of transfer as the Internet from the scope of the data protection Directive. The data protection commissioners, meeting in the Article 29 group, have also 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 shortly and posted in the europa website.

j) 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.

k) 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?

---

[2] Commission decision 2001/497/EC in OJ L 181 of 4.7.2001, page 19. Available also on our website: europa.eu.int/comm/privacy

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.

l) *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 they can enforce their rights and that they are entitled to redress if they suffer damage or distress as a result of a breach of these principles. We are conscious of the need to avoid procedures for implementing Articles 25 which are exclusively unilateral. Third countries concerned need to be informed and given the chance to express their views.

(extract from Directive 95/46)

CHAPTER IV: TRANSFER OF PERSONAL DATA TO THIRD COUNTRIES

Article 25 : Principles

1. The Member States shall provide that the transfer to a third country of personal data which are undergoing processing or are intended for processing after transfer may take place only if, without prejudice to compliance with the national provisions adopted pursuant to the other provisions of this Directive, the third country in question ensures an adequate level of protection.

2. The adequacy of the level of protection afforded by a third country shall be assessed in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations; particular consideration shall be given to the nature of the data, the purpose and duration of the proposed processing operation or operations, the country of origin and country of final destination, the rules of law, both general and sectoral, in force in the third country in question and the professional rules and security measures which are complied with in that country.

3. The Member States and the Commission shall inform each other of cases where they consider that a third country does not ensure an adequate level of protection within the meaning of paragraph 2.

4. Where the Commission finds, under the procedure provided for in Article 31 (2), that a third country does not ensure an adequate level of protection within the meaning of paragraph 2 of this Article, Member States shall take the measures necessary to prevent any transfer of data of the same type to the third country in question.

5. At the appropriate time, the Commission shall enter into negotiations with a view to remedying the situation resulting from the finding made pursuant to paragraph 4.

6. The Commission may find, in accordance with the procedure referred to in Article 31 (2), that a third country ensures an adequate level of protection within the meaning of paragraph 2 of this Article, by reason of its domestic law or of the international commitments it has entered into, particularly upon conclusion of the negotiations referred to in paragraph 5, for the protection of the private lives and basic freedoms and rights of individuals. Member States shall take the measures necessary to comply with the Commission's decision.

Article 26 : Derogations

1. By way of derogation from Article 25 and save where otherwise provided by domestic law governing particular cases, Member States shall provide that a transfer or a set of transfers of personal data to a third country which does not ensure an adequate level of protection within the meaning of Article 25 (2) may take place on condition that:

(a) the data subject has given his consent unambiguously to the proposed transfer; or

(b) the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of precontractual measures taken in response to the data subject's request; or

(c) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and a third party; or

(d) the transfer is necessary or legally required on important public interest grounds, or for the establishment, exercise or defence of legal claims; or

(e) the transfer is necessary in order to protect the vital interests of the data subject; or

(f) the transfer is made from a register which according to laws or regulations is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate legitimate interest, to the extent that the conditions laid down in law for consultation are fulfilled in the particular case.

2. Without prejudice to paragraph 1, a Member State may authorize a transfer or a set of transfers of personal data to a third country which does not ensure an adequate level of protection within the meaning of Article 25 (2), where the controller adduces adequate safeguards with respect to the protection of the privacy and fundamental rights and freedoms of individuals and as regards the exercise of the corresponding rights; such safeguards may in particular result from appropriate contractual clauses.

3. The Member State shall inform the Commission and the other Member States of the authorizations it grants pursuant to paragraph 2.

If a Member State or the Commission objects on justified grounds involving the protection of the privacy and fundamental rights and freedoms of individuals, the Commission shall take appropriate measures in accordance with the procedure laid down in Article 31 (2).

Member States shall take the necessary measures to comply with the Commission's decision.

4. Where the Commission decides, in accordance with the procedure referred to in Article 31 (2), that certain standard contractual clauses offer sufficient safeguards as required by paragraph 2, Member States shall take the necessary measures to comply with the Commission's decision.