EUROPEAN COMMISSION
DIRECTORATE GENERAL XV
Internal Market and Financial Services
Free movement of information, company law and financial information
Free movement of information and data protection, including international aspects

XV D/5020/97-EN final
WP4

WORKING PARTY ON THE PROTECTION OF INDIVIDUALS WITH REGARD TO THE PROCESSING OF PERSONAL DATA

First orientations on Transfers of Personal Data to Third Countries - Possible Ways Forward in Assessing Adequacy

Discussion Document adopted by the Working Party on 26 June 1997

Reflections on Transfers of Personal Data to Third Countries - Possible Ways Forward in Assessing Adequacy

1. Introduction

This document does not aim to address all of the issues arising under the directive in connection with transfers of personal data to third countries, but rather seeks to focus on the central question of assessing *adequacy* in the sense of Article 25, paragraphs (1) and (2). The scope of the exemptions to the requirement of 'adequate protection' contained in Article 26(1) are not considered at all here. The working assumption is that the wording of these exemptions is fairly narrow, and that there are likely to be large numbers of cases which fall outside their scope and which are therefore subject to the adequacy test. The Working Party will seek to examine the precise scope of these exceptions in future work.

It should not be forgotten that the term *adequate* is also employed in Article 26(2), which envisages the possibility of *ad hoc* solutions, notably of a contractual nature, for situations where there is an absence of adequate protection in the sense of Article 25 (2). Procedurally, however, the directive deals with these cases very differently. Whereas under Article 25 Member States are required to notify each other and the Commission in cases where adequate protection has *not* been ensured and the transfer has therefore been blocked, under Article 26 the obligation is reversed, with Member States required to inform the Commission and other Member States of each authorization granted. This reflects the fact that such contractual solutions have inherent problems, such as the difficulty of a data subject enforcing his rights under a contract to which he is not himself a party, and that they are therefore appropriate only in certain specific, and probably relatively rare, circumstances. The Working Party will seek to examine separately the circumstances in which *ad hoc* contractual solutions may be appropriate, and set out some principles as to the possible form and content of such solutions in future work. In substance this work is likely to draw significantly on the ideas set down in this document, given that a test of *adequacy* is as much a feature of Article 26(2) as of Article 25 (1) and (2).

2. Procedural Issues

Article 25 envisages a case by case approach whereby the assessment of adequacy is in relation to individual transfers or individual categories of transfers. Nevertheless it is clear that, given the huge number of transfers of personal data leaving the Community on a daily basis and the multitude of actors involved in such transfers, no Member State, whatever the system it chooses to implement Article 25[1], will be able to ensure that each and every case is examined in detail. This does not of course mean that no cases will be examined in detail, but rather that mechanisms will need to be developed which rationalise the decision-making process for large numbers of cases, allowing

[1] Member States may set down different administrative procedures to discharge their obligations under Article 25. These may include imposing a direct obligation on data controllers and/or developing systems of prior authorisation or ex post facto verification by the supervisory authority.

decisions, or at least provisional decisions, to be made without undue difficulty or excessive resource implications. Such rationalisation is needed irrespective of who is making the decision, whether it be the data controller, the supervisory authority, or some other body established by Member State procedure.

(i) White Lists

An obvious mechanism for such rationalisation would be the development of a 'white list' of third countries which can be assumed to ensure an adequate level of protection. Such a list could be 'provisional' or 'for guidance only', and therefore without prejudice to particular cases which might present particular difficulties. Nevertheless, to be consistent with the overall approach of Article 25, it would be important to ground any decision for inclusion of a country in a white list on the basis of individual cases, rather than a simplified and abstract appreciation of a legal text. Once several representative cases of transfers to a particular third country had been considered, and in each of them it had been judged that the protection afforded was adequate, the country in question could be 'white listed'.

One difficulty of this approach is that many third countries do not have uniform protection in all economic sectors. For instance many countries have data protection law in the public sector but not in the private. In the United States the situation is even more complex, in that specific laws exist for certain particular areas, such as credit reporting and video rental records, but not in others. An added difficulty occurs for countries which have federal constitutions such as the US and Canada, where differences often exist between the various states that make up the federation. In view of this difficulty, care would need to be taken in deciding whether the protection afforded to a particular data transfer was representative of the entire country or only of a particular sector or state. Nothing would prevent the partial white listing of a third country, and indeed, for transfers of data from Spain, distinctions are made already under existing national law between countries assuring protection across the board and those assuring protection only in the public sector.

A further question arises as to who should make the decision regarding inclusion in such a list. It should be noted in this regard that the Article 29 group has no explicit role in making decisions about particular data transfers. This role is carried out by the Member States in the first instance, and then the Commission under the Comitology procedure laid down in Article 31. However, as stated above, any work of the Group would be intended to provide guidance regarding a broad mass of cases, and not necessarily as a means of determining a particular case. It should also be recalled that one of the specific duties of the Article 29 group is to give the Commission an opinion on the level of protection in third countries. It therefore falls well within the remit of the Article 29 group to examine the situation in particular third countries in the light of some individual cases, and come to a provisional view as to the adequacy of the protection. Where such decisions are positive they could constitute parts of the white list envisaged. The list could then be distributed widely and used by data controllers, supervisory authorities and Member States as a guide to their own decisions.

Where a country is not included in such a white list, this need not imply that the country is implicitly 'black-listed', but rather that no general guidance regarding that particular country is yet available. The establishment of an explicit black-list of countries, even if for the purposes of guidance, would be politically very sensitive.

(ii) Risk analysis of specific transfers

Although the establishment of a provisional white list of third countries would be a valuable aid to the decision-making process in respect of large numbers of data transfers, there will nevertheless still be many cases where the third country in question does not feature on the white list. How Member States deal with these cases may well vary according to the way Article 25 is transposed into national law (see footnote on the previous page). If a specific role is given to the supervisory authority either to authorize data transfers before they take place, or to carry out an *ex post facto* check, the shear volume of transfers involved may mean that a system to prioritise the efforts of the supervisory authority will need to be envisaged. Such a system could take the form of an agreed set of criteria which enable a particular transfer or category of transfer to be considered as posing a particular threat to individual privacy.

The effect of such a system would not be to change the obligation on each Member State to ensure that only those transfers where the third country ensures an adequate level of protection are permitted to take place. The fact that a transfer does not pose a particular threat would not remove the basic requirement of Article 25 for adequate protection to be secured. However, the degree of risk to the data subject that the transfer involves will provide a useful guide in helping to determine the precise nature of what is considered to be 'adequate protection'. The system would also constitute guidance regarding which cases of data transfer should be considered as 'priority cases' for examination or even investigation, and thereby allow the resources employed to 'police' the system to be directed towards those transfers which raise the greatest concerns in terms of the protection of data subjects.

The Working Party will produce a specific and more detailed paper outlining the categories of transfer which it considers pose particular risks to privacy. However it is likely that such categories would include the following:

- those transfers involving certain sensitive categories of data as defined by Article 8 of the directive;
- transfers which carry the risk of financial loss (e.g. credit card payments over the Internet);
- transfers carrying a risk to personal safety;
- transfers made for the purposes of making a decision which significantly affects the individual (such as recruitment or promotion decisions, the granting of credit, etc.);
- transfers which carry a risk of serious embarrassment or tarnishing of an individual's reputation;
- transfers which may result in specific actions which constitute a significant intrusion into an individual's private life, such as unsolicited telephone calls;
- repetitive transfers involving massive volumes of data (such as transactional data processed over telecomunications networks, the Internet etc.);

- transfers involving the collection of data in a particularly covert or clandestine manner (e.g. Internet cookies).

3. What constitutes 'adequate protection'?

The purpose of data protection is to afford protection to the individual about whom data are processed. This is typically achieved through a combination of rights for the data subject and obligations on those who process data, or who exercise control over such processing. The obligations and rights set down in directive 95/46/EC are based on those set down in Council of Europe Convention N°108 (1981), which in turn are not dissimilar from those included in the OECD guidelines (1980) or the UN guidelines (1990). It would therefore appear that there is a degree of consensus as to the content of data protection rules which stretches well beyond the fifteen states of the Community.

However, data protection rules only contribute to the protection of individuals if they are followed in practice. It is therefore necessary to consider not only the content of rules applicable to personal data transferred to a third country, but also the procedural mechanisms in place to ensure the effectiveness of such rules. In Europe, the tendency historically has been for data protection rules to be embodied in law, which has provided the possibility for non-compliance to be sanctioned and for individuals to be given a right to redress. Furthermore such laws have generally included additional procedural mechanisms, such as the establishment of supervisory authorities with monitoring and complaint investigation functions. These procedural aspects are reflected in directive 95/46/EC, with its provisions on liabilities, sanctions, remedies, supervisory authorities and notification. However outside of the community it is less common to find such procedural means for ensuring compliance with data protection rules. Parties to Convention 108 are required to embody the principles of data protection in law, but there is no requirement for additional mechanisms such as a supervisory authority. The OECD guidelines, meanwhile, carry only the requirement that they be 'taken into account' in domestic legislation, and thus guarantee no procedural means at all to ensure that the guidelines actually result in effective protection for individuals. The later UN guidelines do, however, include provisions on supervision and sanctions, which reflects a growing realisation worldwide of the need to see data protection rules properly enforced.

Against this background it is clear that any meaningful analysis of adequate protection must comprise the two basic elements : the content of the rules applicable, and the means for ensuring their effective application.

Using directive 95/46/EC as a starting point, and bearing in mind the provisions of other international data protection texts, it should be possible to arrive at a 'core' of data protection 'content' principles and 'procedural/enforcement' requirements, compliance with which could be seen as a minimum requirement for protection to be considered adequate. Such a minimum list should not be set in stone. In some instances there will be a need to add to the list, while for others it may even be possible to reduce the list of requirements. The degree of risk that the transfer poses to the data

subject (see Section 2(ii) above) will be an important factor in determining the precise requirements of a particular case. Despite this proviso, the compilation of a basic list of minimum conditions is a useful starting point for any analysis.

(i) Content Principles

It is suggested that the basic principles to be included are the following:

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. The only exemptions to this rule would be those necessary in a democratic society on one of the grounds listed in Article 13 of the directive.

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. The only exemptions permitted should be in line with the Articles 11(2) and 13 of the directive.

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. The only exemptions to these rights should be in line with Article 13 of the directive.

6) restrictions on onward transfers to other third countries - further transfers of the personal data from the destination third country to another third country should be permitted only where the second third country also affords an adequate level of protection. The only exceptions permitted should be in line with Article 26 of the directive

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

1) **sensitive data -** where 'sensitive' categories of data are involved (those listed in article 8), 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 transferred 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 transfer is the taking of an automated decision in the sense of Article 15 of the directive, 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.

(ii) Procedural/ Enforcement Mechanisms

In Europe there is broad agreement that data protection principles should be embodied in law. There is also broad agreement that a system of 'external supervision' in the form of an independent authority is a necessary feature of a data protection compliance system. It is not sufficient, however, to simply state, without any form of reasoning or justification, that these two features are in some way inherently necessary for protection to be adequate. To do so would be to draw up purely formalistic criteria for evaluating this question.

It is suggested that a better starting point is to seek to identify the underlying objectives of a data protection procedural system, and on this basis to judge the variety of different judicial and non-judicial procedural mechanisms used in third countries in terms of their ability to meet these objectives.

The objectives of a data protection system are essentially threefold:

1) to deliver a **good level of compliance** with the rules. (No system can guarantee 100% compliance, but some are better than others). A good system is generally characterised by a high degree of awareness among data controllers of their obligations, and among data subjects of their rights and the means of exercising them. The existence of effective and dissuasive sanctions is important in ensuring respect for rules, as of course are systems of direct verification by authorities, auditors, or independent data protection officials.

2) to provide **support and help 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 institutional mechanism allowing independent investigation of complaints.

3) to provide **appropriate redress** to the injured party where rules are not complied with. This is a key element which must involve a system of independent arbitration which allows compensation to be paid and sanctions imposed where appropriate.

4. Applying the theory in practice

(i) Countries that have ratified Council of Europe Convention 108

Convention 108 is the only existing instrument of international law in the data protection field other than the directive. Most of the parties to the Convention are also Member States of the European Union (all 15 have now ratified it) or countries, such as Norway and Iceland, which may in any case be bound by the directive by virtue of the European Economic Area agreement. However, Slovenia has also ratified the Convention, and other third countries, such as Switzerland, may do so in the near future. It is therefore of more than purely academic interest to examine whether countries that have ratified the Convention can be considered to afford an adequate level of protection in the sense of Article 25 of the directive.

Such an examination should ultimately be undertaken, as pointed out in section 2 of this document, by looking at a number of specific cases. However, as a starting point it is nevertheless useful to examine the text of the Convention itself in the light of the theoretical outline of 'adequate protection' set out in the previous section of this document.

As regards the content of the basic principles, the Convention could be said to include the first five of the six 'minimum conditions'. [2] The Convention also includes the requirement for appropriate safeguards for sensitive data which should be a requirement for adequacy whenever these such data are involved.

The missing element of the Convention in terms of the content of its substantive rules is the absence of restrictions on transfers to countries not party to it. This creates the risk that a Convention 108 country could be used as a 'staging post' in a data transfer from the Community to a further third country with entirely inadequate protection levels.

The second aspect of 'adequate protection' concerns the procedural mechanisms in place to ensure that the basic principles are rendered effective. The Convention requires its principles to be embodied in domestic law and that appropriate sanctions and remedies for violations of these principles be established. This should be sufficient to ensure a reasonable level of compliance with the rules and appropriate redress to data subjects where the rules are not complied with (objectives (1) and (3) of a data protection compliance system). However, the Convention does not oblige contracting parties to establish institutional mechanisms allowing the independent investigation of complaints, although in practice ratifying countries have generally done so. This is a weakness in that without such institutional mechanisms appropriate support and help to individual data subjects in the exercise of their rights (objective (2)) may not be guaranteed.

[2] There may be some slight doubts about the 'transparency principle'. Article 8 (a) of the Convention may not equate to the *active* duty to provide information which is the essence of Articles 10 and 11 of the directive.

This brief analysis seems to indicate that transfers of personal data to countries that have ratified Convention 108 could be presumed to be allowable under Article 25(1) of the directive provided that

- the country in question also has appropriate institutional mechanisms, such as an independent supervisory authority with appropriate powers; and
- the country in question is the final destination of the transfer and not an intermediary country through which the data are transitting.

Of course this is a rather simplified and superficial examination of the Convention. Specific cases of data transfers to Convention countries may raise new problems not considered here.

(ii) Other cases

Clearly the vast majority of data transfers from the European Union are to third countries which have not ratified Convention 108. In these cases where no binding instrument of international law is applicable, there is no alternative but to return to the basic approach of this paper, i.e. to draw conclusions about the adequacy of the level of protection afforded in a third country on the basis of the situation arising in one or several specific cases. An evaluation of a particular data transfer can sometimes then be considered as valid for broad categories of analogous cases. Analysis of such highly representative transfers will facilitate the development of a provisional white list of countries or sectors within countries.

It would appear that three types of transfer would be possible under the directive:
1) a communication of personal data by a data controller based in the Community to another data controller based in a third country;
2) a communication of personal data by a data controller based in the Community to a processor in a third country processing on behalf of the community-based controller;
3) a communication of personal data by a data subject based in the community to a data controller based in a third country.

The 'core principles' set out in Section 3 are likely to apply in different ways to these three different types of transfer. For example, the classic situation where a transfer is made by a data controller based in the Community to a separate data controller in a third country is by its nature very different to a case where data are collected directly by a data controller based outside of the Community from an individual data subject in the Community, via the telephone or over the Internet.