Methods for EU to assess adequacy put to the test

The assessment of what can be regarded as adequate protection in transborder data flows keeps occupying the European Commission. An answer needs to found in the next ten months. A preparatory method of assessment will be tested during a study of data transfers in six non-European countries.

For countries outside the European Union, a provision of the EU Data Protection Directive that causes serious concern is the requirement for adequate protection of personal data in transborder data flows.

The EU Data Protection Directive (Article 25) determines that personal data may be transferred to countries outside the EU only if they provide an adequate level of data protection. This applies both to personal data already processed in a Member State, and data that would be processed only after the transfer.

The difficult issue is determining what is meant by "adequacy." A Data Protection Working Group was set up last year to tackle this and other co-ordination, interpretation and implementation issues. The group consists of Data Protection Commissioners of different Member States and a representative of the European Commission, Dr. Ulf Brühann, who is Head of Unit at Directorate General XV. This Article 29 Group which was created as an advisory body under Article 29 of the Directive, (PL&B October '97 pp. 7,8) needs to complete its work by the Directive's implementation deadline, 24th October 1998.

The same timetable applies to the Committee consisting of representatives of the Member States and the Commission set up under Article 31 of the Directive. Both the Working Group and the Committee have an official role in making decisions regarding data transfers to third countries outside the EU.

"White lists" a starting point

Last summer, the Data Protection Working Group published its first views on possible ways of assessing adequacy *(First Orientations on Transfers of Personal Data to Third Countries - Possible Ways Forward in Assessing Adequacy).* The document recognises that it will be impossible to examine all transborder data flows in detail, but nevertheless there should be a mechanism for a rational decision-making process which can be adopted regardless of the body making the decision.

An easy option would be to determine which countries have adequate data protection. However, difficulties arise as there are countries which may have adequate protection in one sector, but not in another. The situation is countries like the United States is even more complicated as data protection provisions vary from one state to another. If a list were compiled, who would decide which countries would be included?

The working group suggests that as it is to give an opinion for the Commission on the level of protection in third countries, it could put together a provisional "white list" for the use of data controllers and Data Protection Authorities. Inclusion on the list would depend on an independent evaluation of cases of data transfers. If a country would seem to have adequate protection in all cases of data transfers studied, it could be included in a "white list."

Risk analysis for countries not appearing on a "white list"

Because the Member States may grant their Data Protection Authorities the right to make prior authorisation of data transfers, the need to prioritise some cases over others will become evident as there is a growth in the number of transfers that need to be examined. The working group envisages that specific attention should be given to transfers of personal data that involve a clear risk to the data subject.

At the moment, the risk categories of data transfers are defined as:

- transfers involving certain *sensitive categories* of data (defined in Article 8 of the Directive)
- transfers which carry the risk of *financial loss* (for example 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)

- transfers which carry a risk of *serious embarrassment* or tarnishing 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
- transfers involving the collection of data in a particularly *covert or clandestine manner* (for example Internet cookies).

Assessment method to be tested soon

This preparatory method of assessing adequacy will soon be tested. The Commission has awarded a contract for a study on the application of the method to five types of data transfers to Australia, Canada, China, Japan, New Zealand and the United States. The transfers that will be studied in each country are in the areas of medical research and epidemiology, management of a human resources database of a multinational company, electronic commerce and global information networks and processing of sensitive data in the context of airline reservation systems. Also, subcontracting agreements will be studied, whereby an enterprise established in the EU has access to an enterprise in a third country for processing personal data.

Contractual arrangements possible

The Directive obliges the Member States and the Commission to inform each other of cases where they consider that a country does not have adequate protection. Similarly, they need to exchange information on any authorisations of data transfers granted. With regard to contractual arrangements, the data protection working group will in the future examine the circumstances in which this solution would be appropriate. It is expected that not many transfers will fall under the exemptions of Article 26, and they will, therefore, need to be examined for adequacy.

Open dialogue with third countries

The European Commission has had discussions with several third countries on transborder data flows. With regard to the United States, the Commission has been particularly concerned about the level of data protection in the health sector, credit reporting and direct marketing.

There have also been discussions with countries lacking data protection altogether. Since data processing costs in some of these countries are considerably lower, the Commission is concerned that these countries might become "data havens" for companies trying to avoid data protection regulations.

Third (non-EU) countries can be divided into those which have ratified the Council of Europe Convention 108 on data protection, and those which have not. It is the view of the European Commission Data Protection Working Group that countries which have ratified the Convention could be seen to have adequate protection provided that they also have independent data protection authorities and that the country in question is the final destination of the transfer.

Therefore countries such as Norway, Iceland, Switzerland and Hungary would seem to fulfil the requirements.

A more formal position on adequacy in transborder data flows is expected before October 1998. On 14th January 1998 the Article 29 Working Group produced a document entitled *Judging industry self-regulation: when does it make a meaningful contribution to the level of data protection in a third country?*

This document will be reported on in a future newsletter.

To obtain the discussion paper of the Data Protection Working Group contact DG XV/D-1.

Tel: + (32) 2 295 1612, Fax: + (32) 2 296 8010
E-mail: D1@dg15.cec.be