OUTCOME OF PROCEEDINGS


No. prev. doc.: 8268/91 ECO 127
No. Cion prop.: 8460/90 ECO 158 - COM(90) 314 final - SYN 287

Subject: Protection of individuals in relation to the processing of personal data in the Community and information security


Chapter VIII - Transfer of Personal data to third countries

I. Situation in the Member States

2. For the preparation of the discussion of Chapter VIII the German and French delegations had submitted written contributions concerning the transfer of data to third countries. These contributions were set out in, respectively, Working Document No 7 and Working Document No 8.

Having introduced and explained their documents a number of other delegations intervened orally to indicate what was the situation in their countries in respect of transfer of personal data to other states.
The Danish delegation explained that two data protection laws existed in Denmark, one concerning the private sector and the other the public sector.

(a) **Private sector**

At national level and as far as the private sector was concerned, a distinction had to be made between sensitive and non-sensitive data. Whereas in the area of sensitive data private firms could not file or communicate such data unless consent had been given or such permission was established expressly by law, non-sensitive data could be filed if it was a natural part of a private firm's activities.

These rules applicable at national level were also to be applied in respect of data to be transferred to other countries.

As regards specifically transfer of sensitive data additional specific rules existed, however, stipulating that such data could not be collected with the purpose of being filed and/or processed in another country.

In Denmark only a few cases concerning transfer of data had arisen concerning particularly statistical data and research data. Such transfer had been allowed on condition that the data had been depersonalised and was used for statistical/research purposes.

(b) **Public sector**

In the public sector no specific data protection rules existed concerning transfer of data to other countries. In special specific legislation, rules did however exist on the passing on of information and in areas not covered by
this special legislation the question of passing on of information was based on an interpretation of the general rule of confidentiality.

It had also been accepted that transfer of data could take place if this was necessary to comply with international obligations.

4. The United Kingdom delegation informed the Working Party that in the United Kingdom the data users had to register and inform the competent authorities where data was sent to. Under certain conditions the competent authority could block the transfer of data and this in the private as well as the public sectors.

Were data to be transferred to a country which was not party to the Council of Europe Convention, there was a possibility to intervene and block the transfer if this transfer would lead to a breach of the data quality principle.

If data were to be transferred to a state party to the Council of Europe Convention the principles of free movement would apply with the possibility however, of intervening if the data were to go on from a state party to the Council of Europe Convention to a state not party to that Convention. If the competent authority intervened it would normally issue a prohibition notice having, however, also the possibility of intervening at an earlier stage and stopping the actual processing of data.

In the United Kingdom few complaints had been made. Whether this was due to the fact that there were no breaches or whether people did not mind that breaches took place, or the damage was limited was however uncertain.
5. The Netherlands delegation indicated that in the Netherlands no specific rules existed in the area of transfer of data to other countries and that the normal data protection rules would be applied.

Until now, as in the United Kingdom, very few complaints had been made and the Netherlands delegation was not aware of problems in the area of transfer of data, even if it was taking place to an increasing extent.

6. The Irish delegation informed the Working Party that in Ireland there was provision in the Irish law that gave the possibility of prohibiting trans-border flow of data. If data were to be submitted to a state party to the Council of Europe Convention, Article 12 of that Convention would be applied, i.e. the transfer would go ahead unless there was a problem of equivalent protection in the state to which the data was to be transferred. If the transfer was to a state not party to the Council of Europe Convention such a transfer would also be permitted unless it would contravene the basic principles of the Convention.

Although Irish law gave the impression that a certain control on the trans-border flow of data could be exercised, it was an unrealistic basis as in practice it was not possible to know when data was transferred to other countries.

7. The Portuguese delegation explained that in Portugal the same basic principles applied to data collection/processing as to transfer of data to another country. Consequently, notification should be made if transfer of data were to take place.

8. The Belgian delegation indicated that the Belgian Bill foresaw that in the public as well as private sectors, it should be declared whether data was intended for export or not. The Bill, furthermore, set out general rules giving the
possibility to regulate the transfer of data. Rules contained in the Bill would also apply to data processed in another country but accessible in Belgium.

9. The Italian delegation informed the Working Party that the Italian Bill on data protection set out a notification system making no distinction between the public and private sectors or sensitive and non-sensitive data.

10. Following the oral explanation given by various delegations of the Member States, the Working Party took note of an introductory explanation by the Representative of the Commission to a note entitled "Trans-border Data flows in a Community Perspective: Points for Consideration", drawn up by the services of the Commission in preparation for the discussions of the Working Party.

II. General discussion

11. Having taken note of the different written information submitted to it and the oral interventions made, the Working Party held a general discussion on the principles which should govern the aspects of trans-border data flow in the Directive.

12. From this discussion two concepts emerged.

A. On the one hand, certain delegations favoured a system where the rule would be the free trans-border data flow providing powers for the competent bodies to intervene under certain circumstances. These delegations argued that, in reality, trans-border data flow took place without anybody knowing about it and that the competent authorities consequently could not evaluate whether the data controllers were disclosing information which should not have been disclosed. Information as to whether trans-border data flow had taken place would only arise if, for example, complaints were made.
In view of the importance of having a free flow of information the Irish delegation suggested that Member States should restrict it only where necessary to protect individuals, i.e. to avoid damage or distress to them or where the communication of the data was a breach of the data protection principles. Accordingly, each Member State, through its data protection authority, should be able to prohibit transfers of personal data to a third country if the transfers were likely to cause damage or distress to individuals because of an inadequate level of protection in that country. The Irish delegation suggested that the Commission, in consultation with the Data Commissioners of the Member States, should issue guidelines to ensure consistency in giving effect to these principles. For example, it would prohibit transfers from anywhere in the Community of any sensitive data originating in a Member State which banned such transfers.

The Irish delegation furthermore suggested that data controllers in the "sending" Member State should be liable for any damage caused to data subjects as a result of transferring the data in the same way as they are liable for damage caused by a breach of the data protection principles. They should also be subject to sanctions in the "sending" Member State, including where appropriate a prohibition on future transfers of data to that country.

As a corollary, data controllers should be obliged to take reasonable care to ensure that damage or distress is not caused to individuals by such transfers.

In the Irish delegation's view the form and method of giving effect to these principles should be left to each Member State and the operation of the provisions would be subject to review after, for example, 5 years.
13. B.

On the other hand a number of delegations warned against a too liberal approach in respect of trans-border data flow. Such an approach would, in these delegation's view, taking into account the ever-increasing trans-border data flow, undermine the whole intention of the Directive. In this context it was mentioned that, for example in the sector of employment agencies, files of candidates for jobs plus police files, from the EC States could be transferred to third states with less stringent rules - combined there - and sent back to the country of origin.

14. C.

The Representative of the Commission, noting that there seemed to be agreement that trans-border flow gave rise to problems, suggested that a distinction be made between the substantive criteria to be applied to such flow and the procedures to be applied in order to monitor that the substantive criteria rules were respected.

15. As far as the substantive criteria was concerned the Commission had, in Article 24 of the draft Directive, proposed an "adequate level" of protection in a third country as the relevant criterion. Looking at this criterion and, for example, the criteria proposed by the Irish delegation, i.e. that the transfer would not be likely to cause distress or damage (see point 12 above), there did not in the view of the Representative of the Commission, seem to be a very big difference.

16. The Representative of the Commission also indicated that a distinction would have to be made between the following four categories of trans-border data flow:
1. flow within commercial organisations (inter-company flow),

2. subcontracting (processing of data in third states),

3. international data network (for example in the bank sector), and

4. commercialisation of data.

17. In order to control the transfer of data different possibilities could, in the view of the Representative of the Commission, be envisaged. Such possibilities could be to make the enterprise transferring data responsible - to provide a system of complaints, notification of transfer or prior agreement. Whatever control system was chosen it was however essential that the system did not differentiate between the Member States of the EC.

18. D.

On the basis of the different interventions made, the Chairman of the Working Party proposed to use in the Directive the criterion "adequate protection in the specific case/sector" for allowing trans-border data flow. This proposal met with the agreement of all delegations.

19. To circumscribe the exact scope of this criterion a definition of adequate protection would, however, be necessary and in this context the Luxembourg delegation suggested preparing such a definition which would be based on the following considerations:

1. the nature of the data;
2. the purpose of the data;
3. period for which data could be considered as being up-to-date.
20. Taking as a starting point that the criteria for trans-border flow would be that of adequate protection in the specific case, the Chairman suggested the following scheme according to which the Commission, assisted either by the Working Party on the Protection of Personal Data or the Advisory Committee, concluded agreements with specific sectors (banks, travel agencies, etc.). These agreements should be completed within a limited time, for example 5 years from the adoption of the Directive or from the date set for its implementation in each Member State.

III. Re-discussion of Article 24 - Principles

Paragraph 1

21. Re-discussing the text of Article 24 paragraph 1 and in response to a question on the inter-relationship between Article 4(1)b and Article 24, the Representative of the Commission indicated that both provisions were necessary in order to embrace the obligations of a sub-contractor (for example, Article 22) operating outside an EC country.

Paragraphs 2 and 4

22. Re-discussing Article 24 paragraph 2 and in response to a question by the Danish delegation as to whether the Commission in the case where it disagreed with a Member State who had forbidden a transfer of data, could oblige that Member State to allow the transfer, the Representative of the Commission explained that the case was not likely to arise. The Commission who ensured the respect of Community law checked whether directives were correctly implemented but did not interfere in the individual application of the Directive. What could happen was, however, that another Member State disagreed with the approach taken by a Member State and brought the case before the Court of Justice.
If, on the other hand, a decision had been taken—in accordance with the procedure laid down in Article 24—that a country did not provide an adequate level of protection and a Member State persistently allowed transfer of data to such a state, the Commission would have to bring the case before the Court of Justice.

Paragraph 3

23. (a) Commenting on paragraph 3 the United Kingdom delegation indicated that a decision as to whether a third state had adequate protection was a serious decision with diplomatic implications. The United Kingdom delegation therefore wondered whether the Advisory Committee established by Article 30 of the draft Directive should not be involved in the decision-making procedure. Several delegations shared the view expressed by the United Kingdom delegation.

(b) Furthermore, in the United Kingdom delegation's view the solution foreseen in paragraph 3 might not be useful and even counterproductive as third states might have sufficient incentive to change their law if they knew that transfer of data would not take place unless they provided for an adequate level of protection. If a provision like that set out in paragraph 3 were, however, to be maintained the United Kingdom delegation preferred that it be separated from Chapter VIII and transferred to the final Chapter of the draft Directive.

Paragraph 5

24. Discussing paragraph 5 it was noted that a number of delegations felt that a provision of a declaratory nature as set out in paragraph 5 would be superfluous.
25. In view of the decision taken by the Working Party about the substantive criteria for allowing the transfer of data to third countries, a number of delegations felt that Article 25 had become redundant. For the German delegation Article 25, which seemed to imply a notification system, was in any event unacceptable.

In the United Kingdom delegation's view it was however premature to conclude that certain derogations should not be provided for even if Article 24 of the draft Directive was amended in light of the Working Party's discussions.

Future Work

26. The Working Party agreed that it would be premature to start a second reading of the Directive and that it would be preferable to concentrate discussions of the Working Party on certain specific outstanding questions. For the next meeting the Presidency will consequently draw up an agenda mentioning the points to be discussed at the meetings of the Working Party in November and December.