20. National law should be allowed to specify *further restrictive conditions*, applying, for example, to *manual processing* and *identity numbers*.
21. The reference in Article 17 (3) to *data concerning criminal convictions* is understood to refer solely to the formal criminal record commonly kept by police or judicial authorities. In that light, no amendment is required to the proposed Article.

Rule-Making Powers of the Commission

22. The need for rule-making powers is strongly doubted.
23. However, where such powers are needed, *full consultation of the Working Party* should be a minimum requirement.

This report is based on a statement of the Data Protection Commissioners' common position, prepared by the host, the Netherlands' Registratiekamer.

THE 1995 INTERNATIONAL DATA TRANSFER CHALLENGE

Assume it is 1995 and the EC directive has now entered into force. It restricts the flow of personal data to countries outside the EC member states which do not have adequate national legislation. How will it affect your organization? Start planning now. The following international personal data transfer scenarios, involving the financial sector, the police, direct marketing and human resources databases, should help you. If you are unsure of the legally appropriate ways to keep the personal data flowing in your case, contact us for further guidance. If you are confident that you have worked out a legal policy, why not test your assumptions on our worldwide readership, by contacting this office with your solution! With your permission, we will publish your proposal, if necessary, anonymously.

Groups of data protection managers from several countries created the scenarios. Did the groups foresee any difficulties and if so, what were their suggested solutions? Professor Brian Napier of the Centre for Commercial Law Studies, Queen Mary and Westfield College, the University of London, provided a commentary aided by his experience as a consultant to the Commission of the European Communities/Council of Europe project on drawing up a model contract designed to ensure equivalent data protection in the context of transborder data flows (PL&B Oct.'91 p.6).

Finance

A UK credit card issuer has a cardholder who uses the card to pay for a flight to Bolivia with Air France; insures himself through a US travel health insurance agency; and buys some souvenirs from a Bolivian shop keeper.

According to the UK's Data Protection Act (DPA), the data user is responsible for data in his control. And the data resulting from the above transactions is considered to be in his control.

The group argued that the data exchange between Air France and the UK card issuer would not give rise to any problems, neither under the EC Directive nor under the DPA. However, the data exchanged with both Bolivia and the US could cause problems because neither country has a privacy protection law or a law which is not considered to be adequate.

The group thought of a very intelligent solution: they proposed a waiver on the reverse of the credit card, saying that the card issuer could not guarantee any form of data protection when the card holder uses his/her card outside EC territory.

Professor Napier commented that he thought this to be a very workable solution. Nevertheless, he wondered how a Data Protection Authority would look upon it.

Police

A US citizen comes to the UK, commits an offence and, before being caught, returns to the USA. Of course, the British police would make enquires with their US counterpart, the FBI, and personal data would be transferred from the UK to the USA.

As the EC draft directive does not cover police data files and police data interchange, this turned out not to be a real case.

Police files were not yet under EC competence, but this might change in the future. The *Draft Resolution of the Representatives of the Governments of the Member States of the European Communities meeting within the Council* asks member states to apply the EC directive to parts of the public sector currently outside the Community's jurisdiction.

After the Lockerbee plane crash, personal data had been transferred to the Isle of Man.

No problems had been encountered in this case.

Is immigration within EC competence?

In principle, immigration falls within the competence of the EC member states. However, the Commission plans to make a proposal on asylum because the member states apparently cannot reach a common position. Professor Napier added that the free movement of workers, as guaranteed by the EC Treaty, can easily overlap with immigration.

Direct Marketing

A US publisher, based in New York, buys data about his chosen market in the UK. The name and address tape is sent to New York for the direct marketing packs to be printed and despatched from there. Is this allowable under the EC directive?

The group thought that it was because by 1995 Congressman Bob Wise's US Data Protection Bill 1991 would be implemented, and thus data protection in the USA would be adequate, as required by Article 24 of the EC Draft Directive.

This answer proved to be incorrect, since the US 1991 Bill does not include the private sector and does not contain enforceable sanctions. Thus the Bill cannot be considered to be adequate.

A US-owned database is established in London. After a time, the data is to be transferred to the USA.

The group thought that this was allowable, because it was a US-owned system. With regard to the data subjects involved, they felt that an opting-out system would suffice to meet data protection requirements.

[NB: One of the proposed amendments to Articles 24-25 of the EC Draft Directive suggests that an adequate level of protection need not be provided in cases where the data subject has given his permission (informed consent) for the export of the data].

Professor Napier made two comments:

1. The DPA was applicable, whether the database was US-owned or not. Accordingly, the argument that export was allowable because it was a US-owned system, did not hold.
2. Regarding the EC draft directive, he doubted whether the opt-out procedure could be equated with "informed consent."

The electoral register in the UK was copied and subsequently processed in the US. Later, the data was to be combined, in Barbados, with lifestyle data.

Again it was clear that nowadays such a case is covered by the DPA, and thus the Data Protection Principles should be complied with. Under the EC Directive the presented case most probably would cause difficulties, as the USA and Barbados lack adequate data protection legislation.

Both Professor Napier and Dr. Malcom Norris, the Isle of Man's Data Protection Registrar, stated that only a case-by-case approach is suitable in the area of transborder data flows. Therefore, more case-law is needed to find out what is acceptable and what is not. One problem is that the UK's Data Protection Tribunal is not a tribunal of record which means that its decisions are not necessarily regarded as legal precedents.

From the Commission's perspective, what is needed is an adequate level of protection as specified in Articles 24-25 of the draft directive. Individual citizens cannot enforce these articles directly, but would do so through their national courts. Also, to derogate from the provisions of Articles 24-25, the consent of the 12 Member States plus the European Commission is needed. Protecting a human right costs money and cannot be seen as an unjustified trade barrier.

Personnel data bases

To legally manage international human resources, the group suggested that a contractual agreement between employee and employer, with worldwide effect, might overcome data protection problems.

Companies are typically attracted by the use of contracts to regulate international transfers of personal data. This is the approach favoured by the International Chamber of Commerce (see p. 2 and PL&B Oct.'91 p. 6).

Professor Napier, in his introduction to the scenario, had already raised three fundamental problems with contractual solutions:

1. Privity of contract which means: how can data subjects benefit from a contract to which they are not partners?
2. If individuals have rights, how do they exercise them? Individuals would need expensive legal aid to fight for their rights against a large company in the EC and its subsidiary or headquarters in a non-EC country to which it is transferring the data.
3. In any case, what should be the content of such a contract?

Professor Napier made reference to Article 14 of the EC Draft Directive which covers rights, such as:

- opposing for legitimate reasons the processing of personal data relating to oneself;
- not to be subject to a decision involving an assessment of one's conduct which has as its sole basis the automatic processing of personal data defining one's profile or personality;
- to know of the existence of a file;
- to obtain access, rectification and erasure.

In his opinion, the additional rights of data subjects as provided for in this Article, could be endangered when making use of such a contractual agreement. Also a Data Protection Authority should study the *use* to be made of the data in the receiving country before it decides on adequacy.

Would it be possible to make the recipient of the data responsible contractually for any further disclosure and/or transmission?

Professor Napier affirmed that this is possible. Even the rights of inspection etc. of the Data Protection Authorities in relation to the data user could be transferred to the recipient in such a way.

This report is based on a session at the Privacy Laws & Business 4th Annual Conference in Cambridge and was written by Dr. A.C.M. Nugter, author of *Transborder Flow of Personal Data Within the EC*, published by Kluwer in the Computer/Law series (PL&B winter 1990/91 p.23).