EUROPEAN DATA PROTECTION COMMISSIONERS PUSH FOR EC DIRECTIVE CHANGES

At the first European Conference of Data Protection Commissioners, held in The Hague in November 1991, they adopted a common view on many aspects of the European Community Data Protection Draft Directive. These views were sent to EC member state governments, the Commission of the European Communities and to the European Parliament's Committee on Legal Affairs and Citizens' Rights.

Scope

1. The Directive should apply to processing by *all natural and legal persons*, except where their activities do not fall within the scope of Community law. The exception in Article 3 (2) (a) for private and personal purposes is acceptable.
2. *Not-for-profit bodies* referred to in Article 3 (2) (b) should not be excluded, but might require specific provisions in a more appropriate chapter of the Directive. In this context, certain exceptions could be provided with regard to notifications.
3. There should not be further exceptions in Article 3 (2) for *press, statutory obligations* etc. Any specific problems raised by these cases should be dealt with separately.
4. *Data collected from public sources* should not be considered as "free data." The principle of finality [purpose limitation] should also apply to files accessible to the public (see The Council of Europe's Recommendation No. R (91) 10 on The Communication to Third Parties of Personal Data Held by Public Bodies).
5. *Back-up files* should be protected, but should not be treated as separate entities from the primary data they are supporting.

Public and Private Sectors

6. The distinction presently made in the directive between *the public and private sectors* should be deleted. Substantive principles covering both sectors have to be defined. Where the processing of personal data is necesary for the execution of a public function or duty, the finality principle [purpose limitation] should be respected.
7. For a definition of *public tasks*, reference is made to the relevant case law of the European Court of Justice and to the relevant case law of the European Court of Human Rights.
8. In other cases, *the processing of personal data should be lawful* only:

   - with *explicit consent* of the data subject, or

   - where necessary for the *execution of a contract* with the data subject, or

   - where necessary for the *fulfillment of a legal obligation*, or

   - where necessary to *safeguard the legitimate interest of the controller*, on condition that the interest of the data subject does not prevail.

   In this context, the term *contract* might also include pre-contractual relationships.

Communication of Personal Data

9. A definition of *third party* would be useful. Data transfer between different legal entities within the same group or falling under the same holding company should be considered as communication to a third party.
10. Communication of personal data to third parties should be lawful on the *same grounds as govern the lawfulness*

of processing and also:

- where necessary to safeguard the *legitimate interest of a third party* or the general public, on condition that the interest of the data subject does not prevail, or

- where necessary to *protect vital interests of the data subject.*

A special note should permit *communication to a processor in order to carry out his functions*, provided that he acts only on the instructions of the controller of the data and maintains proper security.

11. Communication of personal data used for special purposes like *direct marketing* might be allowed under certain conditions, which need further study. The same applies to communication of personal data for *research and statistical purposes.*

Information to the Data Subject

12. The Directive should guarantee sufficient transparency of data processing for data subjects and the general public. Individuals from whom personal data is collected should have the *right to be informed without request* of the matters stated in Article 13.
13. Data subjects should be informed of the matters stated in Article 9, *at the latest, at the time of first communication,* in all cases where they cannot reasonably be expected to be aware of the fact that data relating to them is being processed, or aware of the nature of the processing.

Notification to Supervisory Bodies

14. Notification should be provided for, to the extent necessary to satisfy the needs for transparency and adequate control by supervisory bodies. Undue bureaucracy should at all times be avoided. Consequently, a *selective approach to notification and subsequent registration*, based on an evaluation of the risks of data processing, is imperative. The distinctions made in the directive are not considered adequate. Data processing for internal use may present risks, whereas a duty to notify in all other cases would be overly bureaucratic. A large *majority of cases should be exempted from notification* either in general or under certain conditions. These conditions could be the subject of specific provisions, standard rules or approved codes of conduct.
15. Exemption from notification would *not imply any exception from other provisions* of the directive.
16. For all remaining cases, *notification and registration with the possibility of later checking* should be considered as the main rule. Member States should be allowed to require *prior checking in certain situations* which present special risks.

Exceptions to the Right of Access

17. Exceptions to the right of access may be required in certain cases, both in the public and in the private sector. In these cases, the *power of supervisory bodies* to carry out the necessary checks is of essential importance.
18. Limitation of this power either falls outside the scope of Community law, or is unacceptable in principle.

Sensitive Data

19. Article 17 of the directive is unrealistic. Explicit and freely given consent is welcomed. Additional safeguards might replace consent in certain specific situations. Whenever *sensitive data is being processed, a higher degree of consent* should be required in relation to the general principles mentioned above.

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.