PREPARE NOW FOR DATA PROTECTION LAWS IN THE 1990'S

Company data protection managers, in addition to complying with current national data protection laws, also need to understand the broad themes underlying them. They also want to gain insights into how the laws are likely to evolve and have an impact on their operations in the future. Ian Walden's report from the Council of Europe's conference in Athens from November 18th-20th last year brings you the highlights from the discussions on problems with the current laws and how the laws could best develop in the light of experience. In particular, how could they be simplified; differentiated according to industrial sectors; incorporate a degree of self-regulation; cope with sensitive data; and respond to electronic surveillance.

A. Common Approaches to Data Protection

Several countries have now amended their data protection laws, for example, Sweden several times, (1976, 1979, 1982 and 1987), Austria in 1986 (see PL&B May '87 p.10) and Denmark in 1987 (see PL&B August '87 p.3). As a result, certain common legislative approaches to data protection issues are becoming clearer, explained Peter Hustinx, Chairman of the Council of Europe Committee of Experts on Data Protection and legal advisor to the Netherlands Ministry of Justice. Indeed, these approaches are also being taken up by several of the latest countries to debate and pass new laws, including the Netherlands (see PL&B May '87 p.18) and Ireland (see PL&B November '87 p.6).

Simplification: The need for simplification has grown in response to the bureaucracy that data protection legislation has brought about, and the corresponding costs and time involved both for business and other sectors. Leading examples of simplified procedures are Austria's more relaxed rules on transborder data flows and the UK Data Protection Registrar's shortened and simplified registration form, specifically designed to help small businesses comply with the law.

Differentiation: The differentiated or sectoral approach to data protection laws has grown from the experience of existing legislation, where general principles have not always adequately dealt with the problems in specific sectors. Tailoring the law to fit the needs of specific sectors can increase the level of data protection for data subjects, and also prevent the creation of unnecessary and unsuitable bureaucratic requirements. For example, in the Netherlands there are separate data protection bills on police records and population files.

Self-regulation: Related to the sectoral approach is the trend towards self-regulation, which is the basis, for example, of the Council of Europe's Recommendation on Direct Marketing (see PL&B August '87 p.16), the new data protection law in Finland (see PL&B May '87 p.14) and the current Netherlands bill (see PL&B May '87 p.18). Groups of data users in each sector are required to draw up enforceable codes of practice. Although this trend was welcomed by some delegates, any consequential weakening of legislation as a result of such codes would be seen as posing a potential threat of weakening data subjects' rights. Several delegates still saw data protection agencies as necessary for effective control. Laws requiring registration of name-linked files were still a useful method of stimulating data users to

think about their reasons for holding information.

Informal sanctions: The consensus was that criminal sanctions are not appropriate in the data protection field, and that it was better to rely on informal and civil law sanctions against data users who were breaking the law. Informal sanctions consist of investigations by the data protection authority where the data user is informed of the complaint and given an opportunity to resolve it. In these situations, data protection authorities may achieve their objectives through the threat and use of publicity, backed by stronger formal sanctions, if necessary.

Legal persons: Some delegates considered that there remained a reasonable case for data protection laws covering legal persons, such as companies and labour unions. Failure to deal with data protection for legal persons in several countries, such as the UK, Sweden and Germany, has left small companies in a grey area regarding the way in which the law covers them. The coverage of legal persons in the data protection laws of several countries, such as Austria, Norway and Luxembourg, had not led to the problems, in particular industrial espionage, that many companies feared when the laws were first passed. The counter argument, that data protection laws should not cover legal persons, is that data protection is a civil rights issue not directly applicable to companies in the same way that it applies to physical persons, and that legal persons are better regulated by company law.

B. Sensitive data

Professor Dr. Spiros Simitis, the Data Protection Commissioner for the German Land (regional government) of Hesse, presented a report on experience of legislating for data that is particularly sensitive, and therefore deserving of greater protection.

The new Greek bill (PL&B May'87 p.6) has followed a growing number of countries, such as Norway and Sweden, in distinguishing between personal data on the one hand and sensitive personal data on the other, with the latter having additional safeguards.

However, Simitis found it impossible to offer any general rule as to what should fall within the "sensitive" category. A common European definition of the term would prove impossible due to:

1. Different national legal traditions concerning the limits of privacy, as well as the differing political-social backgrounds to organizations such as labour unions. Such differences in circumstances also operate within the state, and Simitis repeated Hustinx's earlier call for a greater stress on the sectoral approach to data protection.

2. An appreciation that no personal information is in reality irrelevant, and to that extent all data can be seen as sensitive.

3. The limitation of certain national laws, for example, Sweden and the UK, to automated data. This limitation is difficult to justify if one supports the Council of Europe principles, which can apply equally to manual records.

Some of the discussion on sensitive data went beyond the classic questions of definition of sensitive data. Two of the questions posed, which would need to be considered in each country where national data protection laws were being introduced or amended, are:

Is a data subject free to choose whether to gain access to sensitive data on himself? "Captive populations" such as prisoners, patients and job applicants may be forced to to use their access rights as part of some administrative requirement. For example, job applicants may be told to gain access to their police files and thus show proof of an absence of a criminal record.

Should a record of data subjects' use of their access rights be seen as sensitive? Simitis told the conference that in the Federal Republic of Germany the police were recording the fact that individuals had made use of their access rights, and including this information on the individual's file.

C. New Information Technologies

Professor Yves Poullet, President of Belgium's Computer Law Association, considered whether the principles laid down in the Council of Europe Convention on data protection were adequate in the face of the growth of new information technologies, and their potential dangers.

Electronic surveillance is one such danger arising from the use of telematic services, for example, automated monitoring of telephone calls, electronic funds transfer at the point of sale, and television viewing patterns (whether or not they are correlated with subsequent purchase data of products advertised on television). In this situation, the individual's privacy is not only vulnerable from the existing sensitive personal data which is stored in a data bank, but also from the personal data which is created from the use of a service or a group of services. Such information gives the file controller a possibility of constructing a profile of every data subject or group of data subjects on the information system.

From File Controller to Network Controller: Poullet also noted that it is important to distinguish data files and their processing location. The growth of computer networks has meant that there is a need for a new terminology, a move from the the concept of the "controller of the file" to that of "controller of the network." The role of the latter would be to take responsibility for all the personal data held on a data subject throughout the network.

Expert systems: Telematic services and expert systems also open up a threat to the Council of Europe data protection principles of data security; the collection of data "fairly and lawfully;" and data being recorded only for "specified purposes." For example, the development of relational databases means that data collected and used mainly for one specified purpose could easily be used in a different way by a different person for another purpose not originally planned.

A right of access to data routes: On a data subject's right of access, further moves are needed towards the transparency of both the

information collected and the routes followed by it in the course of operation. For example, in certain cases, it would be desirable to track when data had been logged into and out of a system. The exercise of a meaningful right of access would therefore need to include a right to monitor the transfer of data throughout the network. This has become increasingly important, especially with the growth of public and private sector networking, and the diversification of some organizations' activities, for example, from retailing to include financial services.

The Equivalence of National Data Protection Laws: Several delegates were concerned about the problem of whether certain national laws were equivalent to others, in particular, the restriction of transborder data flows due to another country not having an equivalent data protection law. Although only a minority of international data flows involve personal data, this was an area that had not been considered in enough detail. For example, does "equivalent protection" under the Council of Europe Convention mean identical or similar protection? In either case, which authority or body will be able to discuss and rule on these issues when such situations occur?

The Consultative Committee, consisting of countries which have ratified the Council of Europe Convention (with other states participating as observers) could serve this purpose. However, so far, it has not addressed such issues of substance. In any case, there are two main problems which weaken this Committee's role:

1. Countries which have not ratified and have not even signed the Convention (for example, the USA and Japan), would not be able to fully participate in these discussions, although they would be greatly affected by them.

2. There are no data protection qualifications for ratifying the Convention and, therefore, becoming a member of the Committee. The most prominent example is the anomalous position of Spain. The other contracting parties to the Council of Europe Convention, France, the Federal Republic of Germany, Luxembourg, Norway, Sweden, and the United Kingdom, will presumably find it difficult at their next meeting in June to treat Spain, with no data protection law, as being equivalent in data protection terms, to other countries with enforceable laws.

Ian Walden is currently carrying out research into data protection with the help of a Council of a Europe Fellowship, and is based in the legal studies department at Trent Polytechnic, Nottingham, in the UK.