MICROCOMPUTING ENCOURAGES NEW STYLE PRIVACY LAWS

Until now, data protection laws have reflected 1970's concerns about the vulnerability of the individual in an era of mainframe computers. Up to, say 1984, there was a fear of records being held by large government departments and large companies processing files on thousands of people, with the ability to link information that had been collected for different purposes. Individuals often either did not know records existed or if they did, data subjects had no rights of access or correction until data protection laws were passed and were enforced.

Since about 1984, huge systems still exist, of course, and the data can be manipulated with increasing ease due to ever more powerful software. But now that microcomputers and their users have grown into millions, data protection authorities face a virtually impossible task of enforcement armed with laws based on a system of mass registration.

Principles OK....

Although there may be a consensus on the validity of the principles of the OECD Guidelines and the Council of Europe Convention, there is a legitimate question of how these principles should be implemented in national legislation. Typical small data bases that could infringe data protection principles are:

* a blacklist of bad tenants kept as a database, available on subscription

* a blacklist of people with a tendency to pursue medical malpractice suits, available on subscription

Organizations offering such services are not necessarily large organizations with operations easily monitored by a data protection authority.

.....But how should they be enforced in law?

Recognizing the needs of individual sectors, the Council of Europe has sectoral working parties. For example, a Recommendation on data protection aspects of direct marketing was approved in 1985 (further details available on request) and the current working parties were listed in the first issue of (PL&B February '87 p.1).

The assumption behind these working parties is that there is a limit to what a law can achieve and that a certain amount of guided self-regulation is necessary to apply common principles to a particular sector.

The conventional legal models

The Sweden's data protection law was the first national law, adopted in 1973, and its mass registration model has been the inspiration of most of the later laws. But it imposes a heavy administrative and enforcement burden on the Data Inspection Board. In contrast, the German data protection law has no federal registration scheme for private companies but puts the obligation on them to adhere to the law. This leads to inconsistent enforcement of the law according to the energy and interest of the Lander authorities and has resulted in more data protection related court cases in Germany than the rest of Europe put together.

The new-style middle way

The teams which drafted Finland's new data protection law and the Netherlands' revised bill have evidently been monitoring these developments. They have, therefore, adopted a fresh approach to national legislation and have skillfully steered a middle way between the Swedish and German systems. They could be fairly described, as indeed they were recently by the OECD's Hans Peter Gassman, as "second generation" data protection laws.

FINLAND FIRST WITH A SECOND GENERATION DATA PROTECTION LAW

Companies operating in Finland should prepare now for the data protection law which was approved by the Finnish legislature on February 4th this year, shortly before the general election, and will come into force on January 1st 1988. After a public debate over several years, the bill took just a year from the time the bill was submitted to the legislature on March 31st 1986 to pass into law. An English translation will be available from about September. All five Nordic countries now have a data protection law.

Scope

The law covers the private and public sectors, automated and manual records and natural persons. Data subjects have the usual rights of access and correction. Companies must give data subjects an opportunity to gain access to records on themselves free of charge at least once a year. If a data subject seeks access more frequently than once a year, then companies may charge the person requesting access only the direct cost. The new law states that the response time to requests should be "without unreasonable delay" which means a maximum of three months.

A two tier system for name-linked data

As it is the government's intention that the law will not be