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

expensive for companies, or for the government, to administer, there is a two tier system according to the sensitivity of the name-linked data.

1. For less sensitive data, the law requires companies to maintain a declaration stating:

* the purpose of an automated name-linked file

* the sources of the data

* the circumstances in which data is transfered to third parties

* uses of the data which are exceptions to the terms of the declaration, a record which must be made available to the Data Protection Ombudsman (DPO) if he makes an investigation

2. But for specific types of name-linked data, companies will need to notify the DPO. In all the following cases, if the DPO is not satisfied with the terms of a company's notification, he will first inform the data user, and ask him to reorganize his data processing on good data protection principles. If he refuses, the DPO will bring the matter to the Data Protection Board (DPB).

The types of name-linked data that must be notified to the DPO are:

Where there is no data user-data subject relationship: For example, unsolicited direct marketing and marketing research data -- but DPO permission will not be needed for scientific research files

For the linking of two or more files: However, if another law states that linking in a particular circumstance is permitted, then the linking is permitted under the data protection law also.

For the export of data For automated data processing or for the large-scale export of data for use in another country. Companies exporting name-linked data to countries which have not ratified the Council of Europe Convention will need to register that fact with the DPO. He would have the power to prohibit or restrict data exports according to the data's sensitivity and the provisions of any data law in the recipient country.

Data processing bureaux must notify the DPO that they are doing this type of work.

Credit information bureaux must also notify the DPO that they are doing this type of work.

The above rules in the law have been amplified in an accompanying decree which was written by the Ministry of Justice and approved by the president at the end of April. It has further

rules for the following sectors:

Marketing information

1. A company may make regular use of a data file on a data subject if it is limited to name, address, age, first language, telephone number, profession or title, and sex.

2. If a company wants to collect information for a specific purpose, it can use additional information, but must destroy this additional information within six months or can ask the DPB to make an exception in particular cases where there are special circumstances.

Scientific and market research, and political opinion polls

Companies may collect, process and store such data without permission from the Data Protection Board if the name-linked data is kept secure and not made public. If a company wished to make the name-linked data public, it would need to obtain an exemption from the DPB.

Companies will be required to destroy the above data after a certain number of years. The Data Protection Ombudsman or Board is expected to draw up guidelines on the types of data that may be stored in archives and the time they should be kept.

Pharmaceutical drug tests

Pharmaceutical companies wishing to test their products may consider the requirement to destroy test data after a certain number of years a problem when they are attempting to track long term effectiveness and patient reactions. They should contact the DPO before starting such a test. As by late May, the DPO has not yet been appointed, companies which need urgent advice should contact the Justice Ministry -- Mrs. Rita Wallin, Law Drafting Department, Ministry of Justice, Riddareg 2B, Box 1, 00131, Helsinki, 17, Finland. Telephone: (358) 0 18251. However, companies should note that a DPO is due to be appointed by October 1st.

Enforcement

The Data Protection Ombudsman (DPO) and the Data Protection Board (DPB) will both be linked with the Ministry of Justice but will be able to take independent decisions.

Enforcement of the law will be based on a three tier system:

1. The DPO, who will begin work on October 1st, will be a full-time appointment and will be supported by about 10 staff. He will publicize the law's principles and requirements, make day-to-day decisions and handle complaints, for example,

people having difficulty exercising their rights of access and correction.

2. The DPB will consist of seven part-time people and will be appointed by the government. They should all have knowledge of name-linked files; at least two will be lawyers and at least two will have experience of data processing. The board will rule on matters of principle submitted to it by the DPO or its own full time secretary. It will be able to impose administrative sanctions, which means financial penalties, to punish those who have infringed the law. It will also be able to permit exemptions from the law under certain circumstances.

In most cases, the DPO will make a recommendation to the DPB. But the DPO will not be a member of the DPB and the DPB will be able to veto DPO decisions.

3. If the DPO is not satisfied by a DPB decision, he can appeal to the Supreme Administrative Court. If he wishes, the DPO may pursue a case through the ordinary courts. An ordinary court would hear a case of damages.

Consistency with international practice

Finland has signed the OECD Guidelines, and its law has been drafted to comply with them. Finland is not a member of the Council of Europe, although the Ministry of Justice has drafted the new law with the intention that it will enable Finland to ratify the Convention after the law is in force. A decision is expected to be taken on this point by the end of 1987.

Timetable

The DPO will start work on October 1st and the data protection law will come into force on January 1st 1988. Companies will have six months to seek any exemptions they require from the DPO. After another six months, January 1st 1989, companies will be required to fulfill all their obligations under the law and will be subject to administrative or judicial sanctions.

Some years later, parliament is expected to review the way the law is working and introduce whatever amendments seem necessary then in the light of experience.