DATA PROTECTION NEWS FROM AROUND THE WORLD

International Organizations

Council of Europe: The Council of Europe has adopted two approaches to data protection issues:

* The sectoral approach: This has resulted in a number of recommendations, including ones on medical data banks; research and statistics; social security records; and direct marketing. The latest one, on police records, was adopted by the Committee of Ministers at Strasbourg on September 17th. The next one, on employment records (PL&B August '87 p.2), is in draft form, but will be passed to a committee of experts in early 1988. The working party on the banking sector (PL&B August '87 p.2) has not yet reached a decision on whether there should be a recommendation on this sector. Texts of recommendations are not available until after they have been approved by the Committee of Ministers.

* There are currently two working parties examining fundamental issues.

1. The first issue is new technology and data protection which for the purpose of the working party covers three main aspects. The first aspect is telemetry, automated measuring, for example, of electricity consumption, and television programmes watched. The second aspect is interactive media like France's minitel system; and the third is electronic mail. The debate on these subjects raises important questions of principle, like whether the concepts of data file and data user are still viable. The consensus is that they are, but they need flexibility of interpretation.

The second issue is the relationship between privacy and freedom of information legislation. The basic distinction between these concepts is that privacy laws give individuals a right of access to records on themselves while freedom of information laws give individuals a right of access to government information in general.

A model which the working party will study, as it combines both freedom of information and privacy in one statute, is Quebec's law on access to documents held by public bodies and the protection of personal information, passed in 1982.

The second meeting of the Consultative Committee, when countries which have ratified the Convention meet to coordinate their policies, is due to be held in June 1988.

Countries with data protection laws

Finland: The new Data Protection Ombudsman (see PL&B May '87 p.14), Rita Wallin, was appointed in October. She was formerly responsible for drafting the Data Protection Act at the Justice Ministry. By March, her team will have increased to about eight people. The address of the Data Protection Ombudsman is: Post Box 31, Helsinki, 931, Finland. Telephone: (358) 0 343 2455.

The Data Protection Ombudsman (DPO) will publicize the law's principles and requirements, make day-to-day decisions and handle complaints. The law will come into force in stages from January 1988. Companies will have six months to seek any exemptions they require from the DPO. After another six months, from January 1st 1989, companies will be required to fulfill all their obligations under the law and will be subject to administrative or judicial sanctions. An English translation of the law is not yet available.

Germany: Dr.Reinhold Baumann, Germany's federal Data Protection Commmissioner reported in Quebec that debt collection companies are now preparing to tackle the Lander data protection authorities on access to the files of the leading credit information organization, SCHUFA.

This is an organization with data on 33 million people in Germany and receives 17 million requests a year for information from its files. Financial institutions are its main shareholders and users. At first, SCHUFA resisted the data protection law restricting its activities. But in 1985, the High Court broke a deadlock between the banks and the Lander data protection authorities and in 1986, the two sides agreed a reform to the system.

1. Use of the data base was limited to lenders. Therefore, data was transferred only to persons who had a justified need.

2. As a result, more than 2,000 companies which had previously gained access to the system, for example, language schools, garages and others, were no longer allowed to do so.

3. The data to be released was limited only to that which was strictly relevant to the purpose of the enquiry.

4. Individual data subjects' access rights were strengthened by enabling them to gain access to records on themselves.

5. Individuals were now able to find out to whom data on them was being transferred, and therefore able to check whether such transfers were justified.

The problem now facing the data protection authorities is that the debt collection companies are not satisfied that they are being excluded from use of the SCHUFA system and are seeking a legal basis for pursuing their claim.

Norway: On November 12th, the Data Inspectorate sent to the Ministry of

Justice an amendment to the data protection regulations covering data security (see PL&B August '87 p.5). This 70 page draft, which could be amended by the Ministry, sets objectives but does not indicate how data controllers should achieve them. It sets criteria by which an organization's data security measures may be assessed for adequacy for data of different levels of sensitivity: 1. not sensitive 2. sensitive 3. very sensitive. The main points in the security regulations are the following:

* Definitions of what is regulated

* Security organization and administration

* Security measures for data processing bureaux, for example, access controls and physical security

* Operational control systems, for example, personnel aspects

* Logical access controls in terms of what they should do, for example:
  - regulate access to the system
  - identify users
  - establish that a user's identity is authentic
  - establish that a user has authorization

* Security of communications networks

* Security measures for media storage and other peripherals

* Security software programs

* Security of the operating system

* Security of data bases

* Physical protection , for example, against flood and fire, and disaster recovery procedures

* Data quality, for example, back-up, accuracy and data sources.

United Kingdom: The UK's Data Protection Registrar accelerated its enforcement effort in late October when the Data Protection Registrar's Head of Investigations, John Lamidey, (see PL&B August '87 pp.8,12) and his team gained a search warrant from the Stafford Court and used it to search the home of a part-time policeman in Burton-on-Trent. This was the first search warrant to be obtained under the Data Protection Act. In doing so, the Data Protection Registrar has made two clear public relations points.

He will act firmly to investigate allegations of police abuse of data. In this case, the Registrar's office had been informed that a policeman was improperly collecting and storing information about other police officers and that he had obtained access to the police national computer and had copied personal data onto tapes and discs at his home.

Secondly, the message should be clear to companies. The data protection

act has teeth and it will bite. In fact, the Registrar has started prosecuting companies which have not registered as required under the act. PL&B will report on the results of these cases in the next issue.

Countries planning data protection laws/rules for companies

Ireland: On October 19th, the Republic of Ireland's Minister of Justice, Gerry Collins, introduced a comprehensive data protection bill into the Dail, (parliament). The new bill covers natural persons and automated data in both the private and public sectors, and has been drafted to comply with the Council of Europe Convention (see page 6 for a full report). The bill is due to have its third reading by being debated in the lower house in the first week of December. The bill could then pass to the upper house, the Senate, shortly afterwards. The new government has given the bill top priority.

The Netherlands: The Netherlands data protection bill (PL&B May '87 p.18) was passed by the lower house of the Netherlands States-General (parliament) on September 8th in the form described by us (see PL&B May '87 p.18). The bill is now before the upper house and it was expected to make its comments to the government in the last week of November. The next stage is for the government to give its response. If necessary this process is repeated. The upper house is then expected to debate the bill around the beginning of February. The upper house may either accept the bill or reject it, but may not amend it. It is expected to accept the current text. The bill should start coming into force in 1988.

New Zealand: Since the Labour government was re-elected in August, the Justice Minister has announced that the government is drafting revisions to its existing data protection legislation. A new data protection law is likely to cover companies and to be supplemented by sectoral codes of practice and regulations.

Currently, New Zealand's law in this area is limited to access to government information (see PL&B Feb '87 p.7). At present, oversight of the legislation is divided between the Information Authority (which has a mandate until March 1988) and the Privacy Commissioner, Mr. P. Molineaux, who has direct jurisdiction over privacy aspects of the Wanganui Computer Centre. This is the main government data processing centre, for the police, the Justice Ministry, the Transport Department and other public bodies.

Privacy Laws and Business will bring you more news from the Quebec Annual Conference of Data Commissioners in the next issue.