DATA PROTECTION NEWS FROM AROUND THE WORLD

International Organizations

Council of Europe: The Netherlands signed the Council of Europe Convention (for the Protection of Individuals with Regard to Automatic Processing of Personal Data) on January 21st, the 18th country to do so (PL&B August '87 p. 20 for the other 17). The only members of the Council of Europe not to have signed the Convention so far are Switzerland, Liechtenstein and Malta.

Luxembourg became the seventh country to ratify the Convention on February 10th. When Luxembourg deposited its ratification, it declared that it would not apply the Convention to:-

a. Data bases which by virtue of a law or regulation are accessible to the public.

b. Data bases which contain data relating exclusively to the owner of the data base.

c. Data bases which have been set up for public international law institutions, for example, the Court of the European Economic Community.

European Economic Community: The EEC is expected to circulate a new draft initiative on data protection within the next few months. To put this forthcoming initative into context, the EEC Commission issued a Recommendation as long ago as 29th July 1981 for member states to introduce domestic data protection laws and sign and ratify the Council of Europe Convention. But it has had only limited success, as seven out of twelve member states have not yet passed data protection laws. However, there are now several factors which are pressing the EEC to take a new initiative:

1. The circulation of information is essential for the growth of the information market and for the free circulation of goods and services. To help create a single internal market by 1992, the Community should seek to reduce divergent national approaches to data protection.

2. Barriers to information flows caused by the lack of equivalent data protection laws are needed to guarantee free flows of data between countries which have ratified the Council of Europe Convention. Some of them, Sweden and Norway, are outside the Community.

3. Another problem with the Council of Europe Convention is that it allows for a number of exceptions. Relying on these exceptions and the different ways that these are applied increases national policy divergences and may have a direct effect on the creation of a single market.

4. Excessive bureaucratic burdens, like telecommunications regulations, may hinder information-based industries.

5. In the context of GATT negotiations the EEC needs an international trade policy for information. This would clarify the conditions and circumstances for giving non-EEC countries access to information within the Community. A

transparent policy would avoid the accusation that the EEC was erecting non-tariff barriers. It would also enable the EEC to demand a similar open policy from other countries, and ensure a guarantee of access to their information markets.

The Organization for Economic Cooperation and Development: The OECD will hold a meeting on May 3rd and 4th to review its member states' attitudes towards (and action on) the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. The meeting will review the results of a questionnaire which it has circulated to member states. So far, the overall response has been that the OECD Guidelines' principles are satisfactory. But some discussion will be needed on a better way to implement the principles in those countries without data protection laws, bills or other provisions.

There may be some role for a formal data protection computer audit analogous to a legally regulated financial audit. This may be a way forward for countries, like the United States, Japan and Australia, without comprehensive data protection laws. They would then have something tangible to offer to satisfy requests for information on their data protection standards from foreign data protection authorities which may be considering restricting the exports of name-linked data.

Countries with data protection laws

Finland: Finland's new Data Protection Ombudsman (DPO), Rita Wallin, explains to PL&B her role and that of the Data Protection Board.

In the six months from January 1st 1988 to the end of June this year, Ms Wallin, helped by two staff - with five more due to begin work in March or April - is advising companies on their obligations under the Data Protection Act. Some companies have clearly not understood these obligations. In the first four weeks of January, of the 30 companies which had sent her notifications of their name-linked data files, only four needed to do so! The DPO has accordingly written orders for companies wishing to use name-linked data for direct marketing purposes or to transfer such data abroad. In these cases, if their applications are not lawful, she writes to the file keepers asking them to make changes to their files or record- keeping procedures as appropriate.

Generally, the DPO can only request organizations to act voluntarily. Much depends on her powers of persuasion. In certain cases, the DPO can issue an order, for example, to ensure data subject access to credit information. In such cases, if the data owner refuses to comply with the DPO's order, the matter passes to the Data Protection Board (DPB).

The DPB has seven members with seven alternates, and it needs a minimum of four to form a quorum. They are from law, data processing, business, labour union and consumer organization backgrounds. Up until the end of January, the DPO had only held meetings at which procedural issues were discussed. The DPO's relationship with the DPB is that the DPO can always send a written submission to the DPB, and attends meetings when she asks the DPB to decide on a question of principle.

Federal Republic of Germany: Draft amendments to Germany's Data

Protection Act were finalised by the Interior Ministry in November 1987 and published in January this year. They will be discussed by interested parties and then will be passed to the Cabinet for a decision on whether (and in what form) the amendments will be submitted to the legislature. The amendments help bring Germany's Data Protection Law more into line with the Council of Europe Convention and include provisions to:

* increase the powers of the Federal Data Protection Commissioner over the public sector.

* order all public sector authorities to cooperate with the Federal Data Protection Commissioner in his efforts to enforce the law.

* give individuals a right to be awarded damages of up to Dm500,000 (£167,225) for violation of their data protection rights.

* require all file owners to store and transfer data only when it is necessary to fulfill the file's objectives.

More details of these legislative proposals will be available in the May issue of Privacy Laws & Business.

Sweden: Sweden's 1973 Data Act's section 23 has been amended by introducing payment of compensation for damage suffered resulting from:

a. the setting up or keeping a personal file without a license or permission required by the Data Act.

b. a person unlawfully gaining access to, altering, deleting or copying an automated name-linked record.

The amendments were adopted on 12th November 1987, the text (SFS 1987:990) was published on 1st December and the amendments will come into force on 1st April this year. Previous amendments were adopted in 1976, 1979, and 1982.

The other group of amendments give the Data Inspection Board authority to issue regulations on the correction of incorrect and misleading data as part of its power under section 6 of the Data Act to grant permission for the setting up and keeping of a personal file. Within this context, it already has power to issue regulations on ten other aspects of file keeping, like the collection of data, the type of data which may be recorded on a file, the notification of data subjects, control and security.

The new amendment to section 8 of the Data Act states: "If there is reason to suspect that personal data in a personal file is incorrect or misleading, the responsible keeper of the file shall, without delay, take reasonable steps to clarify the matter." An item of incorrect or misleading data shall be corrected, modified or deleted, which will have the effect of minimising risk to the data subject's privacy.

"If any item that is corrected, changed or deleted has been disclosed to anyone other than the data subject, the responsible keeper of the file shall notify the recipient of the data about the correction, modification or deletion, if requested by the data subject or if there is risk of the data

subject's privacy being invaded."

"A data subject who has reported that he considers that data on him is incorrect or misleading shall be notified of the action that has been taken as a result."

"The responsible keeper of the file shall appoint one or more people to assist data subjects when data is thought to be incorrect or misleading and to notify them of any corrective action taken. The responsible file keeper shall make available to the public the names of the people who have been appointed for this task."

"The provisions of this section do not apply to a personal file received by a public records authority for archiving. The Data Inspection Board may exempt the responsible keeper of the file from complying with this section."

In a separate regulation, passed on 4th January 1988, and published on 21st January, the Data Inspection Board extended its supervisory powers to automated data processing on audits carried out by the tax assessment authorities. This regulation came into force on 1st February this year.

The Data Inspection Board has also recently issued new regulations on the use of personal data files for direct marketing purposes (see p.16).

United Kingdom: As reported in the last two issues of Privacy Laws & Business (August '87 p.12 and November '87 p.4) the Data Protection Registrar has now started prosecuting organizations and individuals which have broken the law. Rosemary Jay, legal advisor to the Registrar, explains how the Registrar and the courts have used their discretion in dealing with the first cases to be brought to court.

1. In December, Alec Norman Garages (Bedford) Ltd, were fined £500 for failing to register under the Data Protection Act [section 5 (1)]. The company pleaded guilty to keeping customer records on computer, but there was no evidence of the company abusing the data or breaching the data protection principles. As a result, and aware that this was the first case brought under this Act, the magistrate imposed less than the maximum fine of £2,000.

2. A prosecution against another garage in Leek, Staffordshire, was abandoned in January this year. The company had automated customer records, but had not registered as it was relying on the accounts exemption. Also, symbols against individual customers' names had apparently never been used. As a result of the investigation, the company agreed to remove the symbols and to register the file.

3. Also in January the Registrar decided not to prosecute the part-time policeman whose home was searched after allegations that he had improperly transferred to his home data from the police national computer. Some of the confiscated tapes were destroyed and some returned. The Registrar decided not to prosecute after studying the Attorney-General's guidelines, but he did make a report to the appropriate police authority.

4. In February, in another case involving the police, the Crown (public)

prosecution service successfully prosecuted an officer under the Criminal Law Act 1977 of conspiring with persons unknown to breach the Data Protection Act. It was alleged that the police officer improperly released the name of a car owner. The reason why the Data Protection Act did not apply directly in this case was that the owner was a limited company and not an identifiable living individual. The policeman pleaded guilty and the Nottingham Crown Court fined him £400.

The simplified registration form for small businesses (PL&B August '87 p.12) has stimulated a fresh flow of applications; over 20,000 in the period from September 1987 to January 1988. Interestingly, the publicity campaign attracted not only 12,500 of the simplified forms but also 8,000 of the original larger forms. By the end of February, there were about 160,000 entries on the register. In addition, by the end of January this year, the Registrar's office had received more than 23,000 requests for changes to their entries. This shows that many organizations are keeping their entries up to date, as they are required to do by the Data Protection Act.

Countries planning data protection laws/rules for companies

Ireland: The Irish data protection bill (PL&B Nov'87 p.6) has now had its second reading in the lower house of the Dail (legislature). A date for its committee stage has not yet been set.

Greece: The Greek data protection bill was laid before parliament in mid-November in the week before the Council of Europe conference in Athens (see page 7). The bill (PL&B May '87 p.6) was discussed in detail at the conference. Two aspects of the bill which received particular comment were:

1. The distinction between the file keeper, the owner of the file who also decides the file's purpose and organization; and the responsible person, upon whom the major liability lies, as this person operates the file and has the power to allow third parties access to it. Some conference delegates considered that this distinction would give companies an opportunity to avoid liability regarding data protection violations.

2. The independence of the Data Protection Commission (DPC). Some delegates feared that the DPC would be too subordinate to the Minister of Justice who has power in the bill to call for a review of any decision of the DPC involving important public interest cases. The Council of Ministers would have final authority to veto any DPC decision if the competent minister could give a good reason for such a decision.

The Netherlands: The Netherlands data protection bill is now moving ahead at a slower pace than expected in November (PL&B Nov '87 p.5). The reason is a number of critical comments in the Upper House's committee reviewing the bill. As the Upper House may either accept the bill or reject it, it is particularly important for the Ministry of Justice to explain and answer any points raised. The comments cover both basic definitions of terms and certain practical points. However, it is still expected that the bill will be passed in the first half of this year, and to come into force either towards the end of 1988 or at the beginning of 1989.