DATA PROTECTION NEWS FROM AROUND THE WORLD

1. International Organizations

Council of Europe: Austria became the eighth country to ratify the Council of Europe Convention (for the Protection of Individuals with Regard to Automatic Processing of Personal Data) on March 30th. When Austria deposited its instrument of ratification, it made some "interpretative declarations" which formally clarified the Austrian government's understanding of certain words and phrases in the Convention and related them to the Austrian Data Protection Act, revised in 1986. In addition, Austria declared that it will apply the Convention to legal persons, to "groups of persons, associations, foundations, companies, corporations, or any other bodies consisting directly or indirectly of individuals whether or not such bodies possess legal personality."

The next countries which are expected to ratify the Convention are Denmark, which has recently amended its legislation to bring it in line with the Convention (PL&B August '87 p.3), and Iceland.

The sectoral working party on employment records, chaired by Vito Librando of Italy's Ministry of Justice, had its draft recommendation provisionally approved by the committee of experts earlier this year. It will pass firstly to the steering committee of legal affairs, the European Committee on Legal Cooperation, and then to the Committee of Ministers, which is expected to approve it in 1989. The draft recommendation covers the collection and use of employee data, like employees' collective as opposed to individual rights; the monitoring of employees by audio-visual techniques; telephone logging; and genetic screening (used, for example, in the nuclear industry to assess individuals' risk of contracting cancer by examining their family medical history).

The Committee of Ministers has now authorized publication of the report of the new technologies working group (PL&B November '87 p.2), which includes a section on expert systems, and will be available within a few months.

Issues which have recently been discussed by the committee of data protection experts include AIDS and press agencies. In future meetings, the committee will deal with data protection related aspects of personal identification numbers and self regulatory codes of practice, also known as "soft law."

The second meeting of the Council of Europe Convention's contracting parties, that is those countries which have ratified the Convention, was held in Strasbourg May 25th to 27th. Other members of the Council of Europe were entitled to attend as observers. The chairman of the meeting was Mme. Charlotte Pitrat, who is the government representative on France's data protection authority, CNIL.

Two of the items on the agenda were:-

1. The interpretation of the concept of "equivalent protection" when referring to the export of name-linked data from countries which have ratified the Council of Europe Convention to those which have not.

The point here is that the Council of Europe Convention, in Article 12.3 a, states that a ratifying state may prohibit the flow of data to another ratifying state or require special authorization where its domestic privacy legislation includes specific regulations for certain categories of data, (for example, data on racial origin or political opinions) unless the other ratifying state provides equivalent protection (PL&B May '87 p.9). In brief, how is equivalent protection to be defined to permit or justify the ban on the transfer of name-linked data from ratifying to non-ratifying countries?

2. The legal status of codes of practice that are used to apply the principles of national data protection laws to specific sectors, like direct marketing (PL&B August '88 p.13).

European Economic Community: The EEC will play a more active role in combatting computer crime, if the Council of Ministers accepts the recommendations of the Legal Advisory Board for the Information Market.

This was the main conclusion from the sixth meeting of the EEC's Legal Advisory Board, which met in Luxembourg on May 4th and 5th. The meeting was called by Directorate-General XIII which covers telecommunications, information industries and innovation. The discussion focussed on a report, The Legal Aspects of Computer Crime and Security, prepared by a team led by Professor Dr. Ulrich Sieber of the University of Bayreuth and Profesor Dr. Guy Vandenberghe of Vrije University, Amsterdam. The report suggested that there are strong reasons for Community action in this area.

To justify a Community initative, the Commission must demonstrate that computer crime is a barrier to the working of the internal market. This would justify EEC action under Article 100, which covers any aspect of creating a unified internal market not dealt with elsewhere. Inevitably, the Community's role in encouraging computerization and the transfer of data between member states will involve the legal and techical aspects of data security. Despite the difficulties of this approach the EEC Commission did not wish to limit its own competence. Ultimately, Community action depends on the political will of the Council of Ministers.

Is this the Single Europe Act??

The Commission could take the following actions:

1. Circulate information on computer crime to raise the awareness of member governments of the extent and seriousness of the issue.

2. Coordinate national laws. If national laws and policies are sufficient, then the Commission can merely support national efforts. This is superficially an attractive route. But some member states regard their criminal law system as an aspect of national sovereignty which they do not wish to surrender to the EEC. In addition, the harmonization of national criminal law does not automatically lead to effective enforcement.

3. Coordinate with other international bodies. Work has already been done in the areas of intellectual property, patents and data protection. Specialised studies, linked with initiatives towards an international recommendation on computer crime, for example, a common list of computer offences, could be a Community responsibility.

4. Assist and encourage member states to ratify the Council of Europe Convention (The Commission is preparing a statement on this point).

5. Coordinate member states' training of police officers and judges on computer crime issues, working where necessary with Interpol.

6. Set up codes of professional conduct or procedure. Terminology would have to be carefully considered because Codes of Practice mean different things to different interest groups and would have to be adapted to specific uses.

The Organization for Economic Cooperation and Development: At a meeting in mid-May in Paris, the member countries of the OECD reviewed the results of a questionnaire. This had been completed by the member states detailing their progress towards complying with the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. There was also a discussion on various sectoral initiatives, in particular, the data protection guidelines of the:

* International Air Transport Association

* Center for Financial Industry Information Systems, Tokyo

* Canadian Bankers' Association

* Society for Worldwide Interbank Financial Telecommunications (SWIFT)

* Société Internationale des Télécommunications Aéeronautiques (SITA).

The discussion centred on whether these codes were effective and whether there was any evidence of the member organizations complying with them. In short, is the self-regulatory approach sufficient? Does it operate as equivalent to national laws?

If any readers, whether companies or data protection authorities, have views on this question, please write to us, as we would like to encourage more public discussion on this important issue.

2. Countries with data protection laws

Canada: This year, the federal government is implementing its plan to extend the Privacy Act (PL&B February '87 p.5 and May '87 p.3). It is adopting some recommendations of the House of Commons' review of both the Privacy Act and the Access to Information Act. The report, published in March 1987 is entitled - Open and Shut: Enhancing the Right to Know and the Right to Privacy. The government's response, - Access and Privacy: The Steps Ahead, was published in October 1987,and promised several initiatives. These included:

1. Extending the Privacy Act to all 53 parent Crown corporations and their 127 wholly owned subsidiaries. Such corporations are owned or financially controlled by the government of Canada. They are involved in transportation, like Air Canada and the Canadian National Railway; communications, like the Canadian Broadcasting Corporation; and energy, like Petro-Canada. As of July 31st 1986, they employed 187,000 people and had total assets of C$55 billion. The government evidently accepted the statement by John Grace, the Privacy Commissioner to the Parliamentary Committee, "Government institutions, because they are governnment, should set the highest standards of privacy protection.....Why should Canada Post be covered by the Privacy Act and not, say, the CNR? Why National Film Board and not the CBC?"

The government has no plans, at present, to extend the Privacy Act to federally regulated bodies, like Canadian chartered banks and cable television companies, and the Privacy Commissioner did not advocate such a policy in his statement to the parliamentary review committee.

2. Establishing a task force, in cooperation with the provincial and territorial governments, to promote the OECD Guidelines throughout the public and private sectors. At the task force's meeting on April 19th, all the provinces were represented, except for Newfoundland. They agreed to develop awareness programmes encouraging the private sector to adopt their own privacy codes. The provincial governments have leverage as they have powers of regulating certain industries within their jurisdictions. In addition the provincial governments own some Crown corporations, like the Liquor Control Board of Ontario (the provincial government has a monopoloy of retail liquor sales in the province) and Ontario Hydro.

3. Studying the implications of the transborder flows of data for the privacy of Canadians, determining whether a problem exists, and if so, addressing it.

4. Giving the go-ahead for the Privacy Commissioner's office to carry out a public awareness campaign to heighten knowledge of the Privacy Act and encourage compliance with the OECD Guidelines in the private sector.

The Canadian Bankers' Association issued a Model Privacy Code on June 12th last year. It is based on the OECD Guidelines and was drawn up in response to the Canadian government's policy of promoting data protection self-regulation in the private sector (PL&B May '87 p.3). The code was presented to the OECD conference reviewing the Guidelines in May.

Finland: The English text of Finland's Personal Data File Act (PL&B May '87 p.14, November '87 p.3, and February '88 p.3) and Personal Data File Decree, which came into force on 1st January 1988, is now available from Privacy Laws & Business. For an overview, see page 19.

Guernsey: The Registrar has so far received over 460 registrations but has not needed to issue any warnings to companies or take any legal action.

Isle of Man: Organizations can now expect faster progress on implementing the Isle of Man's Data Protection Act, passed on July 16th 1986 (PL&B August '87 p.4). The reason is that the Isle of Man's government has recently appointed its first Data Protection Registrar whose office opened on April 22nd. His name and address are:

Dr. Malcolm Norris, Isle of Man Data Protection Registrar, P.O. Box 69, Douglas, Isle of Man. Telephone: 0624-26262.

His first decision will be the date or dates for bringing the Act into force. The timetable for implementing the Act, as laid down in section 41, may have to be shortened. The appointed day for registration is likely to be in the fourth quarter this year. Application forms are not yet available. The exemption for small businesses (PL&B August '87 p.4) is intended to allow them to use their accounts as a means of providing mailing lists for their existing customers. But it is not clear at this stage how workable this provision will be. For example, there is not yet a clear definition of a small business.

Jersey: Since our report last year (PL&B August '87 p.4), Jersey has appointed a Data Protection Registrar. He is:

Mr. G. R. Sidaway, Data Protection Registrar, Data Protection Registry, c/o Judicial Greffe, Royal Court Chambers, 10, Hill Street, St. Helier, Jersey, United Kingdom. Telephone: 0534-32273.

So far, some 600 applications have either been registered or are being considered for registration. Each application costs £20. Guideline booklets and application forms are available from the Registrar. Although the Registrar is frequently in contact with companies, he has not yet needed to issue any warnings or take any legal action.

United Kingdom: Eric Howe, the Data Protection Registrar, circulated a consultation document in late May reviewing the working of the Data Protection Act, and has asked for replies by August 1st. He explains, "I

shall use the replies as a basis for reaching conclusions on possible useful amendments to the legislation. I shall in due course report these conclusions to Parliament and bring them to the attention of ministers." He is assuming that "the practical way is to seek to amend the Act in order to make it work better rather than to start completely afresh."

One issue that has already been raised involves a management-labour data protection conflict which is not resolved by the current Act. The question is whether an employer may exert pressure on job applicants to exercise their rights to gain access to their police records so that the employer can see them. The Registrar comments that "To use the Act to force individuals to find and reveal information about themselves is contrary to the objectives of data protection and should be stopped. If public policy requires the disclosure and exchange of information about individuals, that should be expressly provided for by legislation."

The Registrar is also interested in obtaining views on how the law might be simplified. Copies of the consultation document may be obtained from:

Mr. Francis Aldhouse, Deputy Data Protection Registrar, Office of the Data Protection Registrar, Springfield House, Water Lane, Wilmslow, Cheshire, SK9 5AX. Telephone: 0625-535 711.

3. Countries planning data protection laws/rules

Greece: Greece's data protection bill (PL&B November '87 p.6) is now being reconsidered by the Justice Minister following last November's Council of Europe conference in Athens. Although the bill is not an issue which divides the political parties, little progress is expected in the near future.

Hong Kong: The Administrative Services and Information Branch of Hong Kong's Government Secretariat wrote in March to computer users to recommend its newly published booklet, Data Protection Principles and Guidelines (see p.14). The letter states that the government has been monitoring international data protection developments, "and has accepted that in principle data protection legislation should be introduced." While deciding which features of foreign legislation are best suited to Hong Kong's needs, the government is introducing the guidelines as an "interim measure." The self-regulatory approach is heavily stressed in the letter signed by P.K.Y. Tsao, the Secretary for Administrative Services and Information:

1. The government "invite(s) your organization's compliance on a voluntary basis."

2. "I have no doubt that as a responsible member of the community you are already following the guidelines and that compliance will not cause you any major problems."

3. ".. the booklet has no legislative effect and.....there will be no enforcement or policing action to ensure compliance."

However, it is clear that the Hong Kong government is preparing the way for legislation covering the private sector. P.K.Y. Tsao tells PL&B that he is currently setting up a working group to examine data protection legislation in other countries to assess what might be most appropriate for Hong Kong. He estimates that Hong Kong's own legislation will be, at least two years away and anticipates that it will cover "both the government and private sectors to safeguard Hong Kong's image as a responsible member of the financial and commercial communities of the world."

Ireland: Ireland's data protection bill (PL&B November '87 p.6) is expected to begin its committee stage in the Dail, the lower house of the Irish Parliament, in the next few weeks. The Minister for Justice, Gerard Collins has tabled several amendments to the bill. The most important ones are analysed on page 17.

The bill may pass to the Senate (the upper house) and be enacted by the summer recess. But if not passed then, the bill will resume its progress in October and become operational six to nine months after being enacted, probably by mid-1989. It is expected that three months before this date, Ireland will ratify the Council of Europe Convention to ensure that the law and the ratification will enter into force at the same time.

Italy: Since the Mirabelli data protection bill was dropped by the Justice Minister about three years ago, two bills have been introduced by members of the parliament but they have made no progress. However, recently, a select committee has been appointed to produce a new bill. The committee, again headed by Mirabelli, consists mainly of judges, law professors and civil servants, several of whom were active in drawing up the former bill. The committee is faced with two main options:

1. Start the drafting process again from the beginning, or

2. Bring the former bill up to date, as it did not cover data bases or personal computers. The committee now considers that it would be unacceptable to require personal computers used for domestic and recreational purposes to be notified to a data protection authority.

The committee is due to report to the government by the end of 1988. Meanwhile, banks and the media are expressing concern over the cost of complying with a data protection law. The fall of the Goria government had no effect on the work of the committee because the justice minister remained the same, and in any case, data protection is not an issue on which the main political parties greatly differ.

Japan: A data protection bill was due to be introduced into the Diet (parliament) on April 28th but was unlikely to be passed in the session due to end on May 25th. However, it is likely that the bill, covering name-linked automated data held by national government agencies, will be carried over to the next session. A literal translation of the bill is "A bill relating to the protection of computer processed personal data held by administrative agencies."

Regarding the private sector, relevant government departments and agencies have been instructed by the cabinet to study the issue. In addition, the government has established a Personal Data Protection Committee in the Consumer Policy section of the prime minister's advisory Social Policy Council.

The background to this initiative is that as of January 1st 1988, there were 393 local authorites with their own data protection laws. However, at the national level, the government had taken its first initiative in this area in January 1976 when it introduced as an administrative measure a Standard Rule for Data Security Related to Computer Utilization. Its aim was to prevent unauthorized disclosure, alteration or destruction of data in national government departments.

In July 1985, the Management and Coordination Agency of the Prime Minister's office established a Study Committee on the Protection of Personal Data. Its report, published in December 1986, concentrated on national government data, as the cabinet had decided in 1984 and 1985 that the appropriate government departments should study the application of data protection principles to the private sector.

The private sector is not simply waiting to be regulated by future data protection legislation. In March this year, Guidelines on the Protection of Personal Data for Financial Institutions were adopted by the Tokyo-based Center for Financial Industry Information Systems. These are a voluntary set of guidelines drafted to comply with the spirit of the OECD Guidelines, and were submitted to the OECD conference in May which reviewed each member states' compliance.

Netherlands: The Netherlands' data protection bill has been delayed by a disagreement over where the Registration Chamber should be located. The government has now decided that it should be sited in the Hague. The Justice Ministry is now preparing a brief to present to the Upper House in June to answer detailed questions raised in its review of the bill. This brief is likely to be discussed in its session in late August or early September. Assuming that the bill is approved at this stage, the law should start to be implemented on January 1st or March 1st 1989.

New Zealand: A data protection bill, is expected to be introduced by the government later this year (PL&B February '87 p.7 and November '87 p.5). It is not clear at this stage whether the government will accept the recommendations of the Information Authority (IA), published on May 5th. The Report of the IA is entitled: - the Collection and Use of Personal Information. The IA recommends that:

1. Personal privacy should be protected by new legislation in the form of additional provisions to the Official Information Act 1982.

2. Identifiable individuals should be covered but not corporate bodies.

3. Privacy rights should extend to both manual and electronically "collected and used information."

4. The Ombudsman should have the power of review of public sector decisions taken under the Official Information Act.

5. The IA's recommendations apply only to the public sector but the report states that its approach is "fully compatible with a more general reform of privacy matters in the private sector, and indeed, provides a timely and significant step in that direction." The IA considers that a general privacy law "presents formidable conceptual and practical problems." However, the IA recommends that "any form of privacy legislation should be based on a generally applicable set of principles." The access and privacy rules should be dealt with by one law and one review body "to eliminate conflict between the reasons for protection and for release."

The IA has now completed its five year task of recommending where the Official Information Act should be expanded in the areas of personal information and will terminate its work at the end of June this year. By mid-May, the government had made no commitment to implement the IA's recommendations.

Spain: The government is giving data protection a low priority in its legislative programme, and has stopped work on its 1985 data protection bill.

Switzerland: Switzerland's revised Data Protection Bill was published on March 23rd and has now been introduced into the Swiss legislature. In June a parliamentary committee will be elected to review the bill. As promised, (PL&B February '87 p.8), we bring you full details in this issue (see p.11). The parliamentary timetable will be decided in the summer. Although there have not yet been any formal reactions to the bill, the issues which are likely to lead to most discussion and delay in adopting the bill are:

1. the role of the Data Protection Comissioner

2. the right of access

3. data protection for legal persons.

At the earliest, the bill could be adopted by 1989. But it is quite likely that there will be a referendum on the bill, in which case, the earliest the bill could be enacted is 1991. So far, there are no plans for Switzerland to sign and ratify the Council of Europe Convention.