DATA PROTECTION NEWS FROM AROUND THE WORLD

1. Countries with data protection laws

Australia: In November, the Commonwealth (Federal) Parliament passed the Privacy Act 1988. The Act applies only to the Commonwealth public sector, and not to State government agencies. The Act also covers the private sector to the extent that it imposes specific controls on companies' use of the Tax File Number. The Privacy Commissioner is given wide delegated legislative powers to prepare enforceable Guidlelines applicable to both public and private sectors. The Act also requires the Privacy Commissioner to encourage companies to adopt the OECD Guidelines voluntarily. It can therefore be considered only a first installment towards Australia's compliance with the OECD Guidelines or eligibility to ratify the Council of Europe Convention. However, it does cover both computerised and manual records. See page 18 for a full report.

Austria: Over the last year, the most significant developments have been as follows:

* There have been amendments to the penal provisions of the 1978 Data Protection Act (section 49) to harmonize them with the new computer crime provisions in the Penal Code dealing with Damage to Stored Data (section 126a Penal Code) and Computer Fraud (section 147a Penal Code). The amendment entered into force on March 1st 1988.

* Court actions on cases involving employment related aspects of the Data Protection Act will from January 1st 1989 be heard in the Labour and Social Courts. This is the result of an amendment to section 29 of the Data Protection Act.

* The Data Protection Commission refused permission for a credit information agency to transfer abroad data about family status because this data was not covered by the legitimate purpose of the agency. The case is now pending before the Supreme Administrative Court.

* The right of access does not include the right to be informed about the source of the data, ruled the Supreme Civil Court in a case on direct marketing and data protection. The court's reason was that the direct marketing company had organized its data in a way which prevented it from identifying the source of the data. This decision may lead to amendment of the law.

Canada: The Privacy Commissioner, John Grace, and his staff together with the Treasury Board and the Department of Justice, have been briefing Crown Corporations on their new obligations under the Privacy Act (PL&B May '88 p.5). By late November, the following Crown Corporations had been briefed: Air Canada, Petro Canada, Via Rail,, Canadian National Railways, the individual ports of St. John's, Halifax, Saint Joan, Quebec City, Montreal, Prince Rupert and Vancouver, Cape Breton Development Corporation, Marine Atlantic Inc., International Centre for Ocean Development, Harbourfront Corporation, Canada Lands Company, (Mirabel, Le Vieux-Port de Québec, le Vieux-Port de Montréal, Canada Museums Construction Corporation Inc., Atomic

Energy of Canada Limited, and Canada Development Investment Corporation.) Some of these corporations have wholly-owned subsidiaries which will also be covered.

The corporations will be added to the schedule of the Privacy Act by Order in Council (an Executive action) rather than by legislative amendment. With the return of the Conservative government under Prime Minister Mulroney in the recent general election, his party's de-regulatory policies may mean that the Privacy Act may not be extended to all Crown Corporations. One possibility is the extension of the Privacy Act only to those Crown Corporations which are not in direct competition with private sector companies. Such a policy would mean that the Privacy Act would not apply to those major Crown corporations, like Air Canada and Petro Canada, which do compete in the private sector (see page 24).

Other changes include:

* the extension of Privacy Act rights to anyone physically present in Canada, rather than being restricted to citizens and permanent residents;

* tightening the definition of personal information about public servants to ensure protection of sensitive data;

* tightening the security policy to enhance protection of personal information;

* improved training for federal government personnel and departmental coordinators;

* a public awareness campaign; and

* an on-line data base for the Personal Information Index, which is the directory of federal government personal information data banks.

Quebec: The Quebec access and privacy law may be extended to certain companies regulated by the provincial government. The Quebec government is now considering whether the Act on access to documents held by public bodies and the protection of personal information should be extended to some of the private sector. Currently, the law, which was passed in 1982 and came into effect in July 1984, covers more than 3,600 public sector bodies, including local government, education and social services.

In October 1987, the Commission on Access to Information presented to the Quebec government its five yearly review of how the law was working. Subsequently, the report was presented to the Quebec Assembly which made its own examination of the Commission's recommendations. One point barely touched on by the Commission but which features in the Assembly's report, is the proposal to extend the protection of name-linked data to the private sector. In the first place, the law might be extended to priority sectors, in particular, credit agencies, insurance companies and banks. It is now for the Quebec government to take a decision.

Denmark: The amendments to Denmark's Public Authorities' Registers Act and Private Registers Act came into effect on April 1st this year (PL&B August '87 p.3, August '88 p.4).

In the public sector, the most important changes are:

* a set of detailed rules must be issued for every computerized name-linked file, except that there is an exemption for files containing little and strictly defined non-sensitive data. However, the general rules of the law still apply to these files.

* The Justice Ministry is currently discussing with central and local government agencies the feasibility of automatically providing data subjects with a printout of files on themselves containing sensitive data. The main issues to be resolved are the level of interest from data subjects and cost to the agencies.

* The Data Protection Agency (DPA) has given guidance to public authorities on the transfer of data to third parties, including other public authorities. Generally, sensitive data should only be disclosed if individuals have given their consent.

In the private sector, the most important changes are:

* general rules, in particular, an explicit right of access by data subjects to computerized files on themselves with access fees determined by the Minister of Justice.

* On consumer credit,

- The data protection authority has had its jurisdiction extended to the transfer of consumer credit data in the banking sector.

- Credit information agencies may only disclose information on debts if: the debt is more than DKr1,000 (£80); and the individual has agreed on the accuracy of the debt information or the case has been brought to court.

- Credit information agencies may only process data by reference to the name of individuals. Access to the information by address is no longer permitted to ensure that creditworthiness is no longer based on such unspecific information.

* On direct marketing,

- The linking of computerized files held by different companies is banned unless the purpose is limited to updating names and addresses. However, the data protection authority may issue a licence to permit other reasons for linking files.

- Companies may not disclose information on consumers to other companies for marketing purposes, unless the company has informed the consumers on the file in writing that the disclosure may occur, and the consumer has given his explicit consent in writing. The Danish data protection authority states that this provision is in accordance with the

Council of Europe's Recommendation on Direct Marketing.

- There are restrictions on the collection of information resulting from telephone marketing.

* On sensitive data:

- Computerized name-linked files containing sensitive data may be set up only after first notifying the DPA. However, this provision does not apply to files kept by associations if the file is intended exclusively for storage of data on members of the association. The DPA has laid down rules on the details of the notification.

- With the approval of the DPA, the Minister of Justice may exempt certain sensitive files from the duty of notification, for example: client files held by lawyers or accountants; patient files held by doctors, nurses, dentists and other such health workers; and personnel files, if filing health data is a duty according to the law or is necessary according to collective agreements on pay.

- Files set up for research and statistics purposes must be notified in advance to the DPA if they contain sensitive data, and the DPA has laid down appropriate safeguards for these files.

* Name-linked information systems held by the press must be notified to the DPA.

* Personal Identification Numbers may be used only if organizations using them comply with the rules on sensitive data.

As a result of these amendments, Denmark will now be able to ratify the Council of Europe Convention.

The amended texts of the Danish data protection legislation are available in English from Privacy Laws & Business.

France: Significant decisions by CNIL, the data protection authority, over the last year relevant to companies include:

* A decision clarifying the use of smart cards for collecting sensitive data. The CNIL approved an experiment to use memory (smart) health cards for people receiving dialysis treatment by the National Federation of Civil Servants and Agents of the State Mutual Fund Societies.

* Enforcement action has been taken mainly against insurance companies.

* A warning was given to the Hermes Association because of the use of a system to detect stolen and lost cheques which violated France's data protection law.

Germany: The Federal Data Protection Commissioner has proposed several amendments to the Federal Data Protection Act, currently being discussed in the legislature:

* One data protection law should cover all forms of automated and manual personal data.

* Data processing should become more transparent by restricting the use of data to its original purpose.

* The Federal Data Protection Commissioner must have sufficient powers, including the right to carry out systematic checks.

* The latest management information systems, like networks, personal computers and image processing, must be taken into account when drafting amendments to the data protection law.

The federal legislature has invited the Federal Data Protection Commissioner to advise a special Committee for the Investigation of the Possibilities and Risks of Genetic Engineering. The Committee has identified a number of data protection issues related to genetics, mainly concerning the collection, storage and use of data, and in particular on:

* the genetic codes of individuals which are collected in the course of ante-natal checks or through the examination of new born babies;

* the health of employees in the context of harmful conditions at their workplace;

* health data on individuals collected to assess their insurance risk;

* data which might serve to link forensic evidence to individuals involved in criminal proceedings.

Ireland: Ireland's Data Protection Act has already been analysed in detail in previous issues (PL&B November '87 p.6, May '88 p.17, and August '88 p.6). The main features of the Act are that it covers automated records, public and private sectors and is a second generation self-regulatory law requiring registration only by specified organizations holding the most sensitive data. This group includes the entire public sector, financial institutions, and agencies dealing with credit information, debt collecting, direct marketing, and computer bureaux. It also includes data controllers holding sensitive data, such as drug testing data on patients, and the health records on workers in food plants or potentially toxic environments, like a chemicals factory. Companies in these sectors in particular will gain a better understanding of their obligations by attending the Privacy Laws & Business conference in Dublin on February 9th.*

Here, we will focus on the timetable for bringing the law into force, as announced by Donal Linehan, the Data Protection Commissioner, at the Privacy Laws & Business conference on October 19th. A copy of his paper is available from the Privacy Laws & Business office.

1. The Data Protection Commissioner was appointed on July 22nd.

2. He then had to establish his office and appoint his staff.

3. The next stage has been the making of regulations, for example, to cover fees, the right of access to health data and the procedures for registration.

4. In December, the Commissioner plans to publish the registration forms together with an explanatory note. There will be five registration forms covering: data controllers and processors, purposes for holding name-linked data, data processing bureaux, amendments to organizations' registration applications, and continuation of registration.

5. In January 1989, registration will begin and continue for a period of three months. Also in January, the Irish government plans to deposit its instrument of ratification for the Council of Europe Convention in Strasbourg.

6. In April 1989, the Act and its regulations will come fully into force together with Ireland's ratification of the Council of Europe Convention.

*** Privacy Laws & Business is organizing, in association with the Confederation of Irish Industry, a conference on Ireland's Data Protection Act in Dublin on February 9th. This conference will focus on companies' obligations under Ireland's Data Protection Act and the registration process. For further details, please contact the Privacy Laws & Business office.**

Luxembourg: The most significant developments over the last year in Luxembourg relevant to companies have been:

* The ratification of the Council of Europe Convention (PL&B February '88 p.2) on February 10th, which came into force on June 1st this year. This has led to the amendment of Luxembourg's data protection law to ban the collection and storage of name-linked data revealing racial origin.

* The data protection Consultative Commission has issued standard rulings for name-linked data held by the banking sector, insurance companies, company accountants, and lists of members. It has waited for the completion of the Council of Europe Recommendation on Employment Records before tackling this sector.

* Robert Biever, President of the Commission since 1982, resigned from his post at the end of 1987 and was replaced by René Faber, Secretary General of Techno-Arbed Luxembourg, who has been a member of the Commission since 1980.

2. Countries planning data protection laws/rules

Netherlands: On November 29th, the Committee of the Upper House of the Netherlands legislature approved the Data Protection Bill (PL&B 'August 88 p.9), which was adopted by the Lower House of the States General on September 8th 1987. It is expected that the bill will be finally approved in a debate in the Upper House scheduled for January 24th 1989. See a full report on page 11.