DATA PROTECTION NEWS FROM AROUND THE WORLD

International Organizations

Council of Europe: The United Kingdom ratified the Council of Europe Convention (for the Protection of Individuals with regard to Automatic Processing of Personal Data) on 26th August, coming into effect on December 1st 1987. As the UK's Data Protection Act comes fully into force on 11th November this year, the UK will be complying with the Convention's provisions by December 1st.

When the UK formally ratified the Convention by depositing its instrument of ratification, it made a declaration (as permitted by Article 3 paragraph 2). The UK stated that it would not apply the Convention to the following categories of automated personal data files:

(a) personal data held only for calculating payroll and pensions or paying deductions from such files

(b) personal data held only for keeping accounts and records of transactions

(c) information which is publicly available under an enacted law.

The UK becomes the sixth country to ratify the Convention after Sweden (September 1982), France (March 1983), Spain (January 1984), Norway (February 1984), and the Federal Republic of Germany (June 1985). The next countries which are expected to ratify the Convention are Austria, Denmark and Luxembourg.

There was a meeting in June of the Council of Europe working party drawing up a draft Recommendation on Personal Data Used for Employment Purposes. This covers the collection, use, storage and communication of data at work (see PL&B February '87 p.1). The next stage will be for the draft Recommendation to be passed to a committee of experts in early 1988. The status of the Recommendation will be the same as that on Direct Marketing adopted in 1985 (see page 16). Recommendations give guidance to: national data protection authorities enforcing national laws; government departments drafting data protection legislation; courts; trade associations drawing up sectoral guidelines; companies; consumer organizations; and other interest groups.

There was also a first meeting in June of a working party reviewing data protection aspects of the banking sector. This covered issues like smart cards, electronic funds transfer at the point of sale, and automatic teller machines. At present, the working party is exploring the following:

* a working definition of banking (to include other financial institutions which transfer money electronically)

* deciding on what they should concentrate (electronic payments rather than consumer or commercial lending)

* the legal status of electronic payments in each country represented.

The working party has not yet taken a a decision on whether to prepare a Recommendation or whether the principles of the Council of Europe Conventiuon are sufficient. Its next meeting is in December.

The Council of Europe is currently drawing up the programme for its conference in Athens on data protection which will be held from November 18th to the 20th this year. It will be an opportunity to review Greece's data protection bill (see PL&B May '87 p.6) as well as wider data protection issues. The Council of Europe held similar conferences in Rome in 1982 and in Madrid in 1984.

United Nations: The United Nations has an interest in data protection issues mainly through two agencies.

1. **The UN Centre on Transnational Corporations (UNCTC),** based in New York (see page 26) is an autonomous body within the UN Secretariat and acts as secretariat to the Commission on Transnational Corporations, a subsidiary body of the UN Economic and Social Council. It has conducted extensive research, published papers and held workshops on various aspects of transborder data flows (TDF) and services and has encouraged some countries, including Brazil, Poland and the Federal Republic of Germany to conduct national studies on the subject. Much of the UNCTC's interest is due to the major role played by transnational corporations in international trade in services, like banking, insurance, tourism, transport, accounting and data services which depend on free flows of international data. The importance of services is that they account for more than half of the value of the economies of the major industrialized countries, represent about half of foreign direct investment flows and nearly one quarter of total world trade. This explains why some companies fear data protection rules as representing a potential barrier to the free flow of data, which would have a negative effect on their operations and the growth of international trade. The UNCTC coordinates the research which will help provide a basis for the new round of GATT negotiations, the Uruguay Round, launched in September 1986, in which services will play a central role. A review of the UNCTC's work in this area and a summary of the Federal Republic of Germany's TDF study is in the Spring issue of the UNCTC's CTC Reporter. A bibliography of the UNCTC's work was published in February 1987 with the title, "UNCTC Work on Services and TDF".

2. **The United Nations Commission on International Trade Law, (UNCITRAL),** based in Vienna (see page 26) last year produced a report, The Legal Implications of Automatic Data Processing, which reviews the work of the major international organizations in this field. It also summarizes their work in areas like privacy, evidence, substitution of data transmission for a written document, use of electronic authentication in place of signature, and liability. UNCITRAL seeks a leading coordinating role in exploring the legal problems that could be expected from the use of computer based communication of trade data.

Countries with data protection laws

Denmark: Denmark's Folketing (parliament) passed the amendments (see PL&B February '87 p.2) in June which will enable it to ratify the Council of Europe Convention. Although the amendments were originally due to come into force on October 1st this year, the date has now been shifted to April

1st 1988. The most important changes in the law are that:

* data subjects will now have an explicit right of access to records on themselves

* companies will have to register sensitive data with the Data Surveillance Agency which will have the right to inspect company property to ensure that the law is being observed

* when companies exchange customer lists, the individuals on the lists will have to be informed.

Guernsey, Isle of Man and Jersey are all off-shore low tax autonomous entities with their own domestic legislation but with the UK handling their defence and foreign affairs. As a result of financial services being a significant factor in their economies and their close relationship with the UK financial community, their data protection legislation is very similar to that in the UK. They have adopted data protection legislation so that they do not become data havens; that is a refuge for data which it would be illegal to process in other countries with data protection laws. By adopting legislation, they have ensured that the UK's ratification of the Council of Europe Convention extends fully to them and avoids the danger of other countries restricting the transfer of name-linked data there.

Guernsey: Guernsey's local parliament (the States of Deliberation) passed its Data Protection Act on July 30th 1986. It was registered on March 3rd 1987, and comes into force on November 11th this year to coincide with the UK Act. Registration of name-linked data files is now taking place and application forms and an information booklet are available from the Data Protection Officer (see page 24). Unlike the UK, Guernsey has no registrar. The Advisory and Finance Committee will oversee the law. It will have discretion, for example, over the number of files that may be covered by each application, costing £22. There will be no tribunal for appeals against its decision, and any litigation will be dealt with by the Royal Court. Within the next few weeks the exemptions for data subject access will be clarified.

Isle of Man: The Isle of Man's local parliament (the Tynwald) passed its Data Protection Act on 16th July 1986. However, no date has been set for bringing the Act into force, a Registrar will not be appointed until next year, no application forms have been prepared and there is no further information available apart from the Act itself. The only significant difference from the UK Act is that the exemptions have been widened to exclude many small businesses from being covered by the Act. The name of the interim data protection official is listed on page 24.

Jersey: Before November 11th, when Jersey's data protection law (PL&B May '87 p.3) comes into force, the States will appoint a part-time Data Protection Registrar, who will eventually be housed in the Judicial Greffe, (Royal Court). The only differences between the Jersey law and the UK's are adjustments to local terminology, although there may ultimately be differences in detailed interpretation. Some large companies are holding seminars for in-house training on data protection. The Acting Registrar, Peter Bryans (see page 24) is currently processing around 400 application forms, which are simpler than the UK's, and estimates that when all small businesses have been included, registrations could reach around 2,000.

Norway: Amendments to Norway's Personal Data Registers Act were passed on June 12th 1987. They come into force on October 1st this year, except for the new telemarketing rules which came into force on July 1st. The text is not yet available in English. The main changes are:

1. Enforcement: A registered keeper of personal data files now has an obligation to help Data Inspectorate staff when they make an inspection visit. Clearly, company personnel could make inspection staff waste a great deal of time if they refused to explain their data processing routines and data security measures.

2. Credit information: Companies will no longer be able to use credit information more than three years old, unless the information is very important for a lending decision. The former time limit was five years, but the new three year limit brings Norway into line with Denmark's law and Sweden's practice. In addition, a new rule is that a credit information agency must inform an individual, if asked, as to who has requested information about him and who has supplied the information.

3. Direct marketing: In July this year the old permits were withdrawn and new conditions were introduced for companies with direct marketing, telemarketing and list-broking operations. The fast growth of laser printing has meant that increasingly personal references can be inserted into direct marketing letters with the consequence that recipients can be more easily offended by messages relating to their precise circumstances or feel that their privacy has been violated. The new rules reflect these concerns:

* Companies planning direct marketing campaigns must now check their files against lists of those who have died to delete these names from their lists. The direct marketing companies were keen to do this anyway, and Readers Digest alone deleted 40,000 names from their lists as a result of this exercise.

* Companies selling by telephone (telemarketing) may no longer use other organization's customer lists.

* Telemarketing is no longer allowed after 9pm (21.00h.) or on Sundays.

* When a telemarketing call is made, the caller must now give his name, his company's name, and the company for which the sales call is being made.

* Individuals now have a right to have their names deleted from direct mail and telemarketing lists.

* There will be advertising on television and in the print media to promote these new rules.

4. Security rules: There is a simplified legal basis for the government to introduce or change data security rules. It will no longer require a change to the law itself. A change in the regulations will now be sufficient. A data security working party is expected to recommend changes to the government next year.

Sweden: Sweden's Datainspektionen (Data Inspection Board) hosted the annual meeting of Nordic data protection authorities in June this year. They discussed: Finland's new data protection law (see PL&B May '87 p.14); the amendments to Denmark's law; moves towards sectoral data protection regulations in Sweden and the experience of the other Nordic countries in this area; and how to make supervision and enforcement of their national laws more effective. Next year's Nordic data protection meeting will be held in Helsinki.

With some 26,500 licenses now issued, Datainspektionen Director-General, Mats Borjesson is now considering ways to reduce the administrative burden of issuing these licenses. He considers that his staff is spending too much time on the issuing of licenses to "responsible keepers" of name-linked data and giving permission for companies to process more sensitive files, as required by Sweden's Data Act. The solution that he is aiming for is a system of general regulations for each relevant sector. If a company meets these conditions, it would then be able to notify, rather than seek the approval of the Datainspektionen, for example, for collecting, storing, using or transferring certain categories of data. The Datainspektionen would still handle any complaints and retain an enforcement role.

Two data processing specialists have been hired this year to help with enforcement work. They will help draw up sectoral regulations in discussion with representative organizations. The first sector that will benefit from this approach will be the municipal health authorities. In the private sector, the first group may be debt collection agencies or companies using direct marketing. Borjesson, in his role as ombudsman under the Debt Recovery Act, receives more privacy related complaints about this sector than any other. The next largest groups of complaints involve credit information and direct marketing.

At some point, the Data Act may well have to be amended to allow for this move toward sectoral regulations. To help parliamentary and wider public understanding of the Datainspektionen's work, an annual report will be published for the first time this October which will, for example, give information on complaints statistics. Most other data protection authorities have always published an annual report.

This development in the Datainspektionen's approach to enforcement has been influenced by the trend toward self-regulation within a framework of law shown most clearly in Finland's new law and the current Netherlands bill (see PL&B May'87 pp.13-22). As Sweden was the first country to pass a national data protection law in 1973, its mass registration system was influential in the way in which other laws were drafted, and several countries, like France and the UK followed this model. Although some countries drafting legislation have kept to a mass registration approach, it is clear that others, like Switzerland, are seeking to have only a minimum of files registered. The rationale is the same as that currently applying in Sweden - to reduce the administrative burden on the data protection authority and focus its enforcement activities on those sectors requiring the most attention.