DATA PROTECTION NEWS FROM AROUND THE WORLD

1. International organizations

Council of Europe: Dr. Joaquim de Seabra Lopes, Director-General of Portugal's Ministry of Justice, was elected chairman of the Council of Europe's Committee of Experts on Data Protection at its March meeting. He replaced Mr. Peter Hustinx, Legal Advisor on Public Law at the Netherlands' Ministry of Justice who served two years as chairman. Also at that meeting the Committee of Experts discussed the Council of Europe Recommendations on employment records, police records and new technologies, the recommendations of the finance working party, plus the latest international data protection news. As the Committee's terms of reference expire at the end of 1989, there was discussion on whether any changes were needed in the years ahead. Any such changes would need to be approved by the Committee of Ministers.

In October, the Committee of Experts will meet again to discuss self-regulation in data protection, personal identification numbers, genetic data, the relationship between open government and privacy legislation, and telecommunications issues.

Transborder data flows, sensitive data, the right of access, and purpose specification were the four main issues discussed when the Council of Europe Convention's Consultative Committee met May 17-19th in Strasbourg. At the meeting were the countries which have ratified the Convention (PL&B February '89 p.17), Austria, France, the Federal Republic of Germany, Luxembourg, Norway, Spain, Sweden and the UK, plus other member countries of the Council of Europe, represented by observers. The individuals who attended were mainly from their national Ministries of Justice but some countries, for example, Austria, Denmark and Ireland were represented by the heads of their Data Protection Authorities.

a) On transborder data flows, the committee decided to try to enaure more transparency and publicity for the factors which need to be fulfilled for the free flow of name-linked data between ratifying countries. This would be achieved by collecting together and publishing:

* all the national declarations on how the Convention is interpreted, for example, extending it to manual files or legal persons.

* all the national legal provisions and policy interpretations which underly the formal declarations.

Surprisingly, there was no discussion on:

* exports of name-linked data to countries which have not ratified the Convention;

* how "equivalent protection" (Council of Europe Convention Art. 12.3 a.) - providing a legal basis for prohibiting transborder flows of personal data - should be interpreted; or

* specific cases which might illustrate national policies.

The committee also took a decision to investigate the establishment of a norm for transborder data flows which would contain minimum information on conditions for the use of the data. The norm would be analagous to those established by the International Standards Organization or one developed for communicating trade data for Electronic Data Interchange (see p.20).

The idea is that any automated export of name-linked data between ratifying countries would be subject to a standard contract on data protection. It would contain a data file indicating, for example:

* the name and address of the recipient of the data;

* authorized uses of the data;

* unauthorized uses of the data;

* recommended storage time for the data; and

* recommended appropriate level of security.

The next step is for the Council of Europe secretariat to study precedents offered by international organizations, like the United Nations Commission on International Trade Law (PL&B August '87 p.3); the United Nations Economic Commission for Europe's Electronic Data Interchange for Administration, Commerce and Transport (EDIFACT); and the International Chamber of Commerce. These precedents will be studied by the Council of Europe's Committee of Experts on Data Protection at its October 3-6 meeting.

b) The Consultative Committee decided that the Council of Europe's secretariat would make a study of each member state's definition of sensitive data, and related policy. This is important because protecting sensitive data is a legal basis for a ratifying country prohibiting the export of data to another contracting party, under Article 12 of the Convention.

c) The third issue discussed was how the right of access is evolving. For example, exercising a right of access to a single file is relatively easy. But when that file has been distributed along a network to several users or branches, each recipient may amend the file which means that there are now several files to which access should be granted to give the data subject a full right of access. Specifically, the meeting agreed that it was vital that the export of data should not deprive individuals of their right of access.

Another problem area is expert systems where data input into the data base is enriched by subsequent use as the software gains "experience." Does a right of access extend only to the raw data, or beyond that to the criteria used by the software for making judgements on individuals, for example, in the context of credit information. Should access be limited only to the raw data, or does it extend to conclusions drawn about an individual?

d) The fourth issue was purpose limitation. This is a principle included in the Council of Europe Convention Article 5 b. "Personal data undergoing

automatic processing shall be...stored for specified and legitimate purposes and not used in a way incompatible with these purposes." This principle is increasingly challenged by the capabilities of relational data bases where uses are not necessarily envisaged when data is collected. Is the concept of purpose limitation, drawn up in the mainframe computer era 10 years ago, still meaningful in the era of personal computers, open networks and distributed processing? Can this principle be enforced? If so, how? It was clear that there were no easy answers to these questions.

The next countries expected to ratify the Convention are: Ireland, the Netherlands, Denmark and Finland, which joined the Council of Europe this year.

The report on the Council of Europe Recommendation on Employment Records has been held over until the next issue of PL&B.

European Economic Community: Legal liability of information service providers was the main subject discussed at the EEC's Legal Advisory Board, (LAB) which met in Luxembourg on May 16-17th. The purpose of the LAB is to help the formulation of policy by Directorate-General 13, which covers Telecommunications, Information Industries and Innovation (PL&B May '88 p.3).

The LAB reviewed the position in each member state on the legal liability of services like hosts and database producers in the event of supplying erroneous information. Part of the discussion dealt with the liability of telecommunication carriers, some of which are currently excluded from liability. There was no consensus in favour of harmonization by the EEC at present. It was agreed that the next LAB meeting on this subject would be held next year and information service providers and users would be invited to attend.

EEC Commission staff are continuing to prepare a policy document on data protection which may be announced at the next meeting of the LAB in October.

2. Countries with data protection laws

Australia: (from Graham Greenleaf, the Privacy Commissioner's special advisor on data protection policy).

Australia's Federal Minister for Consumer Affairs, Senator Nick Bolkus, announced in April that the Australian federal government would introduce national legislation to control credit reporting practices. One option under consideration is that the Privacy Commissioner would be given the function of administering the new legislation.

The decision was announced at a "Summit Meeting on Credit Reporting" called by the Privacy Foundation, a private lobby group. Those attending the meeting included the Privacy Commissioner, federal senators, representatives of the New South Wales Privacy Committee, the credit industry, and consumer and welfare groups. The announcement is in response to the plan by Australia's monopoly credit information body, the Credit Reference

Association of Australia (CRAA) to introduce "positive reporting." This new programme would expand the bureau's function from merely reporting credit defaults to also recording the monthly payment performance of every credit holder.

Kevin O'Connor, the Privacy Commissioner, has written to PL&B with an update on our previous report (PL&B February '89 p.3).

1. The Australian government has now increased his staff allocation to 20 and his operational budget for the year 1989/90 is $Aust 1.9 million. (Nigel Waters, Assistant Registar at the UK Data Protection Registrar's office, will shortly be joining the Australian Privacy Commission as a senior member of its staff).

2. The government recently introduced legislation into Parliament which would extend the Privacy Commissioner's jurisdiction to include a spent convictions scheme. This bill is similar to the UK's Rehabilitation of Offenders' Act and deals with issues like the length of time a conviction may remain on an individual's record - ten years is proposed for an adult.

3. His correct address and telecommunications numbers are: Mr. Kevin O'Connor, Privacy Commissioner, Human Rights And Equal Opportunity Commission, Level 24, American Express Building,

Postal Address: GPO Box 5218, Sydney, NSW, 2001, Australia.

Street Address: 388 George Street, Sydney, NSW, 2000, Australia.

Telephone: 229 7600 Fax: 229 7611 Telex: AA178000 DX 869 Sydney

The Australian judicial case report scheduled for this issue has been held over as the law has now been modified by a subsequent case.

Canada: Federal Privacy Commissioner, John Grace, hosted a "Privacy Summit" at his Ottawa office on February 22nd for senior members of his staff together with Sidney Linden, Ontario's Information and Privacy Commissioner and Jacques O'Bready, President of Quebec's Access to Information Commission and their senior staffs. The purpose of the meeting was to exchange information and to explore the possiblity of joint research and joint policy submissions to government on privacy issues of common interest. Their discussion covered the confidentiality of medical records; the Federal Privacy Commissioner's policy statement on AIDS (PL&B February '89 p.4), which has since been published; computer matching controls; and the use of the Social Insurance Number (PL&B February '89 p.4). Finally, they discussed the extent to which the private sector would develop privacy codes without being required to do so by the government (PL&B August '88 p.22).

Denmark: The number of requests for advice and complaints to the Data Surveillance Authority (DSA) about the private sector in 1988 were:

* Sensitive data (S. 2(3) - research & statistics	205
* Business and trade associations	92
* Blacklists	74
* Credit information bureaux	60
* General enquiries on interpreting the law	54
* Sensitive data (S. 3(4) - mainly insurance)	38
* Headhunters and recruitment agencies	29
* Data processing bureaux	8
* Direct mail agencies	7
* Data processing abroad	1
Total	568

Of these 568 references to the DSA, 140 (25%) were complaints. Of the 140 complaints, 41 (29%) were on credit information. Of the 41 complaints on credit information, the DSA considered that 30 (73%) were justified.

France: The Commission Nationale de l'Informatique et des Libertés (CNIL) reports that by the end of 1987, after the law had been in force for eight years for the private sector and nine years for the public sector, there were a total of 146,626 simplified registrations and 17,487 ordinary registrations. In the private sector, the overwhelming majority of the registrations are of the simplified type. In 1987, the latest year for which statistics are available, CNIL received:

* 1,172 requests for advice

* 3,798 ordinary registrations

* 15,266 simplified registrations

If a data user refuses access or correction to a data subject, the data subject may appeal to CNIL, which will investigate the problem. In 1987, there were 1,132 references and complaints to CNIL concerning:

* direct access to records (563);

* complaints (365);

* requests for advice (117); and

* indirect access mainly relating to the Ministries of Interior and Defence (87).

The greatest category of reference to CNIL concerned direct marketing and the press (424), compared with employment (157), and insurance, banks and credit (82).

Germany: Dr. A. Einwag, Federal Data Protection Commissioner, has corrected our report on the proposed amendments to Germany's Federal Data Protection Act (PL&B February '89 p. 5). There is no plan to restrict the law to automated records. Both the proposals put forward by the Federal Government and the draft bill prepared by the opposition, recognise the need for the law to cover both automated and non-automated records. To restrict

the law to automated records would contradict the principle stated in the judgement of the Federal Constitutional Court on data protection in the census case. (PL&B February '87 p. 3).

Dr. Ulrich Dammann, a senior staff member of the federal Data Protection Commissioner's office, has written the following report on proposed amendments to Germany's Data Protection Act. (It has been translated into English by PL&B):

On February 10th, the Upper House of the legislature, representing the 11 Federal regions, debated the federal government's draft bill for amending the Data Protection Act and made many important suggestions for further amending it, for example to:

1. provide appropriate legislation for the processing of manual files by companies. Currently, the data protection law applies only to manual data bases but not to other manual files;

2. widen the definition of data to take into account recent developments in information technology, and not restrict it to any specific form of processing;

3. regulate the use of files by bringing it within the Data Protection Act. The use of data is currently excluded from the Act;

4. introduce for the first time a right to claim compensation for damages. At present, data subjects may claim for compensation only under general provisions of the civil law.

5. strengthen the rights of individuals harmed in private sector data processing.

The government's bill and the Upper House's suggested amendments will be discussed by the Interior Committee of the Lower house in June, and again in the autumn. As there is disagreement within the government coalition on many issues of data protection rights, it is impossible to predict whether or when the above amendments will pass into law.

Ireland: By April 19th, the deadline for registration under Ireland's Data Protection Act, (PL&B February '89 pp.5,10), the office of the Data Protection Commissioner had received around 1,100 applications for registration followed by another 100 in May. By late May, the Commissioner's office was continuing to receive registrations and handling enquiries from potential registrants. The Commissioner's policy at present is to continue accepting applications for registration recognizing that many organizations have genuine problems in properly completing the forms.

By late April the numbers of registering organizations from each sector were as follows:

Public including health authorities (350); financial institutions (70); insurance companies (90); pharmacies (150); other commercial and

business operations (150); credit unions (180); voluntary health and advice agencies (50); hospitals (24); doctors/dentists (50); churches (4); and political parties (2).

The most common problems reported to the Commissioner's office are:

* A false assumption that universal registration is required, as in the UK and France;

* Complaints about lack of access to personal information held by credit reporting companies and banks.

In the future, the Commissioner will organize publicity about the right of access, and later will turn his attention to working with trade and professional associations to help them draft sectoral codes of practice.

Isle of Man: By April 17th the deadline for the six month registration period, the Data Protection Registrar's office had received around 500 registrations out of around 1,200 registration packs sent to interested organizations. Late registrations are still being received. But organizations suspected of processing automated name-linked data which have not yet registered, like banks, will receive reminders shortly. Dr. Malcolm Norris, the Data Protection Registrar, urges all companies which should register to do so, as they are currently technically in breach of the Data Protection Act, and in due course he will be obliged to take further action. He and his staff are currently processing the registrations they have received so far. He points out that registrations received without a signature and cheque are invalid. Apart from registrations, he is also starting to deal with complaints on data protection issues.

In April, the Data Protection Registrar moved his office to the upper floor of Willow House, Main Road, Onchan, where the new Onchan Public Library is situated. However, his address and telephone number remain the same: Dr. Malcolm Norris, Data Protection Registrar, ODPR, PO Box 69, Douglas, Isle of Man. Telephone: 0624 661030 International: (+44) 624 661030.

Norway: Georg Apenes will become the Data Inspectorate's (DI) new Director from October 1st this year. He is a member of the Storting (legislature) and serves on the Justice Committee which reviews the amendments to legislation. He, therefore, has previous experience of the Personal Data Registers Act. He has worked as a lawyer and journalist, and replaces Helge Seip, who is retiring on reaching the age of 70, after some 10 years as director.

From January 1st 1989, specific regulations have applied to credit information services, data processing agencies, opinion poll and market research companies, and addressing and distribution services. The Storting (legislature) decided in December 1988 that the DI should collect an annual fee of NKr3,000 (£260) from companies in all these sectors. There are an estimated 400 companies in Norway which should pay this annual fee. The fee is to enable the DI to recruit three new staff to more effectively control

these companies' activities. The addition of one data processing specialist and two lawyers brings the total DI staff to 14.

The DI's annual report for 1988 states that complaints and requests for advice which the DI received from individuals, the public and the private sectors totalled some 2,290 last year. It also handled 810 license applications and export notifications last year. Of this total there were 84 export notifications, all from the private sector. The largest percentage rise in license applications came from the public sector with an increase of over 75% from 247 in 1987 to 439 in 1988. The DI now has a total of around 16,000 licenses and notifications on its files.

The DI's annual report for 1988 gives some examples of cases where permission has been granted and refused, both of which give insight into the DI's policies. Permission to operate automated processing of name-linked data was given in the following cases:

* A credit card company, American Express, was permitted to keep an automated file of the telephone numbers called by its card holders using Comvik Card Call credit card telephones. In principle, the DI does not like telephone logging but has given permission for its use under specified conditions for hotels. In this case, the company argued that it could not collect its debts without the call information. The DI accepted this argument.

* A toll station in Trondheim may keep an automated file of vehicles passing the toll station with the drivers'/owners' consent. But if the individual drivers/owners refuse, automated files may not be kept.

Permission to operate automated processing of name-linked data was refused in the following four cases:

* An access control system which depended on keeping an automated record of encoded fingerprints linked to a file of individuals entitled to enter a building was refused permission. The decision for the Identix company was that it was acceptable to have fingerprints encoded in plastic cards to have them checked against the card holder's fingerprints. But it was unacceptable to link the fingerprints with a data base of individuals permitted access to a building. The DI feared that the encoded fingerprints linked to a name file would in time enable them to develop the same status as a Personal Identification Number.

(In contrast, Denmark's data protection authority has accepted the company's request to link the encoded fingerprints to the names of the individuals to whom they belong).

* A proposed administrative system to assist unemployed young people in the town of Grimstad aimed to collect information on all those aged 18-24. The project involved collecting information for the departments of Social Affairs, Social Security and Labour. The DI initially refused permission because the project planned to collect too much information. Later, the DI gave permission on certain conditions, like obtaining data subjects' informed consent.

* A research project on pupils who were not attending their schools was refused permission because the principle of informed consent had been neglected.

* The fourth case was a system for evaluating the capabilities and needs of mentally disabled people for administrative purposes. The rejection was on the grounds that too much detailed information was being collected.

Sweden: By March 31 1989, 33,000 file keepers were registered with the Data Inspection Board.

* In the year July 1st 1987 to June 30th 1988 there were around 2,500 applications for a license to operate more sensitive files, a category which includes credit information.

* There were 552 complaints in the year July 1st 1987 to June 30th 1988. The largest categories related to debt collecting and consumer credit information.

United Kingdom: The Data Protection Registrar's office is preparing a new guidance note to expand on note no. 19, Fair Obtaining - Notification issued last August (PL&B February '89 p.7). Its main emphasis will be that where data users have not informed a data subject of how data on him will be used, the data user may in some circumstances need to approach the data subject a second time to inform him that data will be used for a certain purpose or for additional purposes. Positive consent will need to be given for using data for additional purposes.

In principle, the simple solution is to inform data subjects when data is being collected of how that data will be used and obtain their consent for that use. However, the Advertising Association's team has reponded to this suggestion by stating that, in practice, there can be difficulties. For example, when individuals respond to offers made on television advertisements, it is difficult to gain their consent for further use of their data.

Any new guidance note published by the Registrar will not be directly enforceable. But if there is a subsequent complaint, the Registrar can issue an enforcement notice. If an organization does not then respond sufficiently within the time allowed by the notice, the Registrar has a basis for a prosecution.

Rosemary Jay, the Data Protection Registrar's legal advisor, has given PL&B an update on the procedures for and status of the Registrar's Enforcement Notices. (The procedure follows guidelines agreed with the Council on Tribunals which regulates most UK tribunals).

Before issuing a formal Enforcement Notice, the Registrar's office serves a preliminary notice, not a statutory notice, which states that the Registrar intends ("is minded") to issue a statutory Enforcement Notice for specified reasons. The letter is sent by recorded delivery and the recipient

is informed that he has 28 days to make a response, which can be in written or oral form. Cases are sometimes resolved as a result of this procedure.

Of seven preliminary notices issued, four have been taken on to a formal Enforcement Notice, two have not, and by late May, one was still being considered. So far, one case, on subject access, has been appealed to the Data Protection Tribunal, and the case is expected to be heard in the autumn. The Tribunal should clarify how subject access should be interpreted which will be beneficial both to the Registrar's office as well as the company involved. This will be the first case heard by the Data Protection Tribunal, and may clarify some of its procedures.

The issues at dispute in these first seven cases which have led to preliminary Enforcement Notices are: subject access; fair obtaining of information; and, accuracy and relevance of data. All companies involved are large organizations, in contrast to the ones prosecuted for not registering (PL&B February '88 p.5).

The Data Protection Registrar's office is winning its prosecutions. Apart from an early case which was withdrawn, the Registrar's office has won the seven other concluded court cases for non-registration under Section 5 of the Data Protection Act. All followed efforts by the Registrar's Investigations Department to persuade the organizations to register, a process described by PL&B (August '87 p.12). The Registrar's office prepares its cases thoroughly and prosecutes in the court nearest to where the offence takes place. The courts are now imposing substantial fines and awarding costs against the prosecuted parties:

* The largest fine so far has been £1,000 with £500 costs;

* On June 2nd this year, an estate agent was fined £500 and had to pay costs of £1,105 at the Bracknell magistrates court;

* Other issues also are now leading to prosecutions. The Registrar's case is waiting for a court date for a prosecution against one organization under Section 6 (6) of the Act on three counts - for "knowingly and recklessly:"

- holding data for an unregistered purpose;
- disclosing data to a person not registered; and
- obtaining data from a source not registered.

3. Countries planning data protection laws/rules

Greece: The Data Protection Bill (PL&B February '89 p.9) has been revised by a different team from the one that drafted it, and was submitted to the legislature earlier this year. However, before the bill could be examined, the legislature was suspended for the general election to be held in June.

Italy: The Commission under Professor Mirabelli is still revising the data protection bill, and is is expected to complete its work and present it to the Minister of Justice by late this year (PL&B May '88 p.8). Meanwhile, on February 21st, the legislature approved Italy's ratification of the Council of Europe Convention on data protection. However, this decision will not lead to Italy formally depositing its ratification at Strasbourg until the data protection bill has been adopted by the legislature.

New Zealand: Geoffrey Palmer, Minister of Justice, said in a speech to the New Zealand EDP Auditors Association on April 18th that the government would take a decision this year on the type of privacy legislation it would introduce. His speech ranged over New Zealand's existing legal provisions covering privacy, like the Wanganui Computer Centre Act 1976 and the Official Information Act 1982 and the advantages and disadvantages of self-regulation in the private sector. Although he gave no indication of the precise form of legislation which would be proposed, he gave a firm indication that he would include the private sector:

> "It would seem essential that both the public and private sector be subject to controls. A unified approach to data privacy is preferable because the conduct and decisions of commercial and professional agencies affect our lives as profoundly as those of state bodies."

Switzerland: Dr Peter Muller, Head of Switzerland's Federal Data Protection Service, informs us that the Data Protection Bill may be weakened as a result of the legislative committee's current study (PL&B May '88 pp.10-13). The committee has met several times this year and has so far considered twenty articles. The main issues which have divided the members of the committee concern the Data Protection Commissioner's jurisdiction in the private sector:

* whether the Data Protection Commissioner should have powers of investigation only in response to data subjects' complaints or whether he should be able to act on his own initiative; and

* whether the Data Protection Commissioner should be able to bring a case to court if his recommendation is not accepted. At present, the text of the bill states that only a person who requests action may pursue his case through the courts.

The next meeting of the legislative committee will take place in September. After their discussion of the bill has been completed, it will be debated in a plenary session of the 1st legislative chamber at the end of 1989 or early next year. Then the bill will pass to the 2nd chamber.

The bill is available from PL&B in French, German and in a full English summary of the provisions which have an impact on business.