DATA PROTECTION NEWS FROM AROUND THE WORLD

1. International Organizations

Council of Europe: Member states are being asked for their reasons for not permitting the export of name-linked data to contracting parties, (that is those countries which have ratified the Council of Europe Convention), and examples of cases where they have forbidden data exports or would do so. This is one of the main results from the the second meeting of the Council of Europe Convention's contracting parties (PL&B May'88 p.3) held in Strasbourg 25th to 27th May. It was attended by Austria, France, Germany, Luxembourg, Norway, Spain, Sweden, and the United Kingdom, plus most of the other member states as observers.

The contracting parties also agreed to prepare guidelines on how member states should interpret the Convention's principles of purpose specification, fair and lawful collection of name-linked data; and data subjects' right of access to records held on themselves.

The draft recommendation of the Council of Europe's working party on employment records (PL&B May'88 p.2) may well be adopted at the Intergovernmental Committee of Experts on Data Protection, in mid-September. From there, it will pass to the steering committee for legal affairs and then to the Committee of Ministers.

The working party on the banking sector (PL&B August '87 p.2) is currently drafting a Recommendation which it will discuss at its next meeting in December. The draft covers both banks and other financial institutions and concentrates on electronic payments like electronic funds transfers at the point of sale (EFTPOS) transactions.

The report of the working party on new technologies (PL&B November '87 p.2) is expected to be published in September. Its title is New Technologies: A Challenge to Privacy Protection? It covers telemetry (the remote collection of data by automated means); interactive media (for example, interactive databases, teleshopping and telebanking); and electronic mail.

The report reviews how each member state's data protection laws cover these technologies. For example, the report identifies those countries, like Norway, with general data protection legislation regulating the way in which telemetry information may be collected. It also quotes the example of the Land of Hesse in Germany which has a data protection law which deals specifically with telemetry and remote monitoring. The law states that organisations using a telemetric system or any other remote monitoring system (for example, measuring electricity consumption), located in an individual's household or place of work must obtain that individual's prior consent. From this review, the report draws up a common list of factors which should be taken into account when regulating telemetry, whether by law or by self-regulatory codes.

The working party is now looking at data protection aspects of expert systems.

Mr. Peter Hustinx, Chairman of the Council of Europe's Committee of Experts on Data Protection, will speak on the role of the Council of Europe at Privacy Laws & Business's conference on October 19th in London.

The Organization for Economic Cooperation and Development: At the OECD meeting of member states in mid-May (PL&B May '88 p.4), discussion focussed on the data protection guidelines of the International Air Transport Association; the Canadian Bankers' Association (see p.22); and the Center for Financial Industry Information Systems, Tokyo (see p.24). Although scheduled, there could be little discussion on the guidelines of the Society for Worldwide Interbank Financial Telecommunications and Société Internationale des Télécommunications Aéronautiques as these organizations did not attend the meeting.

There was **no consensus on the three codes that** were discussed. Arguments against were that:

* codes without legal backing had little value;

* there was no guarantee that the codes would be implemented by the member organizations;

* there were some important omissions, for example, none of these codes have provisions for data subjects to take complaints to an independent industry ombudsman.

Arguments in favour of the codes were that:

* in the absence of legislation in many countries, the codes at least show an awareness and acknowledgement of data protection issues;

* they represent a publicly declared intent to protect the interests of data subjects

* they provide a standard by which their members' operations may be judged.

There was much discussion on whether codes are sufficiently equivalent to national laws and how both might evolve in the future. As data protection is just part of the OECD's work in the computer and telecommunications area (much attention these days is given to telecommunications standards and tariffs), some representatives saw future developments growing from concern over data network security.

There is debate, for example in the USA, over whether new telecommunications legislation should make eavesdropping (listening in) on network communications an offence. This broadens the data protection debate beyond the narrow confines of name-linked records to a wider interpretation of privacy but serves to strengthen the case for high standards of data management.

This approach to data protection may be seen as merely corporate self-interest but that interest may converge with European legislation approaching data protection from a more regulatory or bureaucratic viewpoint.

For example, in North America, in the absence of comprehensive data protection legislation covering the private sector, the attention of corporate top management is most easily drawn to data protection issues through vulnerability to threats like hacking and computer viruses (computer programs which cause all or some of its host system to malfunction or be destroyed completely). As corporate top management becomes more aware of their company's dependence on computer systems so they become more interested in independent audits of their computer security and in devising measures to combat these threats. Such audits could include, for example, assessing the accuracy, relevance, and security of name-linked files; in effect a check on the company's adherence to the OECD's Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.

The convergence with the latest European data protection legislation is that the second generation of legislation puts greater emphasis on corporate self-regulation within the framework of law. Therefore, companies in Europe will be increasingly motivated by self-interest and the demands of law, both pushing in the same direction. This explains the great interest at the OECD meeting in Finland's new law (see p.4) which incorporates these new principles, and the way it is being enforced.

Although there is weight to this argument, some representatives stated firmly that whilst the traditional European approach may be seen as too legalistic and expensive, legislation is still needed to raise the awareness of data owners to their responsibilities to maintain high standards in complying with data protection principles. In short, if there is no legal requirement, the job of data protection will not be done.

2. Countries with data protection laws

Denmark: English translations of the revised Public and Private Registers Acts (PL&B August '88 p.3) have recently been completed and are now available from our office. Denmark will soon ratify the Council of Europe Convention.

Finland: When Finland's Personal Data Files Act first came into force on January 1st this year, Finland's Data Protection Ombudsman (DPO), Rita Wallin, explained her role and that of the Data Protection Board (PL&B February '88 p.3). Last year, we described how the law would work (PL&B May' 87 p.14) and in our last issue, we gave an overview of the structuure of the law and its decree (PL&B May '88 p.19). Now that the first six month period of notification is finished, we asked her about her enforcement work.

In the January to June period, the DPO received about 200 notifications of name-linked files, mainly from credit information companies and data processing bureaux. Some direct marketing companies have already submitted their notifications, although they have until the end of December this year to do so.

Ms. Wallin received about 100 written complaints since January and a few hundred more by telephone. The DPO and her eight staff have been active in trying to resolve these complaints by taking up cases with the relevant organizations. The DPO will not name such companies at this stage, as she

wants to encourage companies to come to her for advice at an early stage of any disagreement with data subjects. Also, as the law is new, there could still be genuine cases of misunderstanding of what the law requires. For example, Ms. Wallin received a complaint about a bank which had collected names and addresses of individuals who were not customers and had used the data for direct marketing purposes without their consent. Ms. Wallin explained to the bank that this was not lawful and the bank destroyed the files voluntarily. If the bank had refused to comply with the DPO's request, the case would have passed to the Data Protection Board (DPB).

Cases which have gone to the DPB include requests to export name-linked data to countries which have not ratified the Council of Europe Convention. Two companies have now received general permission to do so, both Finnish direct marketing companies. They are:

* Malar, which applied to export data to Belgium, the Netherlands, Italy, Canada, Switzerland, the USA, Austria and Luxembourg, (the last two before they had ratified the Convention;)

* Pica Data Base, which applied to export data to Belgium, the Netherlands (which have not passed a law and have not ratified the Convention), Denmark (which has passed a law but which has not yet ratified the Convention) and the UK, Norway, Sweden, and Germany (which have all ratifed the Convention, and therefore the application to the DPB was unnecessary for export to these countries).

The authorization procedure which the DPB adopted was to require the recipient organizations in the non-ratifying countries to make a declaration to the Finnish exporting companies that they would respect the data protection principles in the Finnish law. The Finnish companies are then required to give a document to the Finnish DPO before they export the data declaring that the data exports comply with the Finnish law. The Finnish companies then have the obligation once a year to inform the DPO of the organizations to which they have exported name-linked data during the past year and to which countries the data has been sent.

In addition to these data export cases, the DPB also has to take decisions on a number of difficult issues where organizations requested exemptions to the law to be granted for particular situations:

* A number of banks asked to keep a common file on individuals who had misused their bank accounts;

* Three cases involve credit information companies which asked whether they would be permitted to include individuals' criminal records as part of their credit records.

* Amnesty International asked whether it could be exempted from sections of the law, as it feared that full compliance with the law would damage the interests of some of the prisoners it was trying to help. (The case of Amnesty International will be discussed on an international basis at September's annual meeting of Data Protection Commissioners in Oslo).

To help companies comply with the law, Ms. Wallin has undertaken an information campaign both through the media and by having five or six

meetings with trade associations representing sectors, such as the banks and direct marketing, which are dependent on name-linked data. Next year, the information campaign will be extended to give data subjects more information about their rights.

Germany: Dr. Alfred Einwag replaced Dr. Reinhold Baumann as Germany's Federal Data Protection Commissioner on 9th June.

Ireland: Ireland's Data Protection Bill (PL&B November '87 p.6) has now passed into law, less than nine months after the Justice Minister Gerry Collins, introduced it into the Dail, the lower house of Ireland's legislature. In a rapid series of moves to beat the summer recess, the bill was passed by the Dail on June 29th; the upper house (Senate) on July 6th; and was signed by the President on July 13th. The amendments analysed in our last issue (PL&B May '88 p.17) were all passed.

An additional amendment was made to Section 13. The original version referred to the Data Protection Commissioner encouraging the preparation and dissemination of codes of practice by trade associations and other bodies. The enacted version goes further by stating that:

1. The Data Protection Commissioner may approve of such a code

2. Any code so approved may be laid by the Minister of Justice before both houses of the legislature. If both houses approve the code, it shall then have the force of law and have the status of a statutory instrument. Such a code cannot diminish data subjects' rights given to them by the Act.

The Data Protection Commissioner was appointed on July 22nd, and is Mr. Donal C. Linehan, who as Principal Officer of the Law Division of Ireland's Department of Justice, was responsible for the work of drafting the legislation. He has also served as his country's representative on the Council of Europe's Committee of Experts on Data Protection. He explained to PL&B that the Act will become fully operational in early 1989. Currently, he is drawing up the regulations to implement the Act and establishing his office. He will give more information on the timetable for companies' obligations and data subjects' rights at Privacy Laws & Business's conference in London on October 19th.

Isle of Man: The Isle of Man is now making much faster progress towards implementing its Data Protection Act, passed two years ago on 16th July 1986 (PL&B May '88 p.6). The appointment of the Isle of Man's Registrar, Dr. Malcolm Norris, in April, has clearly acted as a catalyst. He explained to PL&B the timetable for implementing the Act. On 12th July this year the Isle of Man's legislature, Tynwald, approved several orders and regulations:

1. The six month registration period will begin on 17th October 1988.

2. All individuals and organizations in the Isle of Man holding or processing personal data must register. The Registrar is taking the Attorney-General's advice on defining the limited exceptions to this rule, and will announce the agreed policy before 17th October.

3. The registration fee will be £23 for each purpose registered multiplied by the number of years, up to a maximum of five, for which the

data user seeks registration. Clearly, this formula makes organizations with complex operations pay proportionately for the number of purposes for which they hold and process name-linked data. The rationale for this policy is to help make the financial contributions of small and large firms more equitable and to help the Isle of Man's Data Protection Registrar's office become self-financing more quickly.

4. Unlike the UK, the information required for registration includes details of the computer hardware and software used, and the organization's business. In particular, the Register entry will require "the make, model and serial number of the data equipment in which the personal data are to be held, or in the case of a network or cluster of data equipment, the data equipment in which the data are normally to be held; the make, name and version number of the program used to manage the personal data; (and) the main business or other activity of the data user for which the data are to be held or used." The reason is that with this information the Registrar will be better prepared to offer advice to data users.

5. The Registrar's office is designing, with the help of a public competition, a logo for use by registered data users to show that they are using personal data "lawfully and responsibly."

6. Data subjects will have a right of access to records on themselves and a right of correction from October 17th 1990.

Dr. Malcolm Norris will be available for answering questions on the Isle of Man's Data Protection Act and its implementation at Privacy Laws & Business's conference on October 19th in London.

Quebec: Mr. Jacques O'Bready was appointed chairman of the Commission d'Accès à l'information du Québec on June 16th, for a five year term. He replaces interim chairman Mme. Thérèse Giroux, who took over from M. Marcel Pépin, host of last year's annual meeting of Data Protection Commissioners.

United Kingdom: A random sample survey of 1,293 data users, commissioned by the Data Protection Registrar published in July, shows that:

1. Larger organizations (more than 500 employees) are most likely to receive enquiries and access requests from data subjects, but mostly from relatively few individuals.

2. A majority of access requests are from employees, which makes it quite easy to respond to requests.

3. Just over a third referred to extra time and work in processing requests, while nearly half reported very little or none. Nearly one fifth spontaneously mentioned positive benefits in that complying with the Act made them rationalise or improve their procedures for handling personal data.

4. Just over a half considered the cost of providing access as a significant or a major concern.

5. Just under half of the companies intend to charge the maximum fee of £10 for access requests, 39% intend to make no charge, while 12% intend to charge less than the maximum fee.

On July 19th, the UK Data Protection Registrar was host to the first meeting between himself and the responsible data protection officials from Guernsey, Mr. Michael Clark; from the Isle of Man, Dr. Malcom Norris; and from Jersey, Mr. Ray Sidaway. Their discussion included:

1. The legislation's implementation in each country;

2. The position of organizations, like major banks, which had registered in the UK but which had branches in these islands. The policy advice is to register in the islands also, either because they must do so in Guernsey and the Isle of Man, or because they may choose to do so to show that they are protecting the interests of the local residents and those with accounts in their branches in Jersey;

3. Defining their policies on payroll and accounts exemptions;

4. Employers asking job applicants to use their rights under the Data Protection legislation to obtain a copy of their records. The consensus was that this is a misuse of the legislation.

Personnel managers in the UK now have practical guidance on how to implement the Data Protection Act regarding automated employee records, following the publication of the Institute of Personnel Managers' (IPM) Employee Data Code, on June 30th. As 85% of the Institute's members now have computerized personnel systems, and a majority of access requests come from employees, the Code will clearly be very useful. It recommends that:

1. Employers should seek to restrict disclosures of information to people outside their firm, even if the disclosure is permitted by the law. For example, if another company asks for information about an employee because he has applied for a job there, his present company should gain the employee's consent before releasing the information.

2. There should be no automatic right for one employee to see another's record, unless the need to know is strictly business based.

3. The Code strongly suggests that employers take the initiative in regularly requesting updates on information from the employees themselves. This policy helps ensure accuracy and minimises the volume of employees' access requests.

4. The Code recommends charging no fee for employee access requests.

The Code was jointly produced by the IPM, the National Computing Centre, the Confederation of British Industry, the Industrial Society and was supervised by the UK Data Protection Registrar. The IPM's Code on Employee Data may be obtained from the IPM, IPM House, Camp Road, Wimbledon, London, SW19 4UW, UK. Price 25 pence.

3. Countries planning data protection laws/rules

Hong Kong: Mr. Peter Harrison, the Senior Administrative Officer responsible for planning Hong Kong's data protection policy (PL&B May '88 pp.7,14), will be available for answering questions on Hong Kong's Data Protection Principles and Guidelines at Privacy Laws & Business's conference on October 19th in London.

Netherlands: There has been another delay to the timetable for the data protection bill (PL&B May'88 p.9). The government brief responding to points raised in the upper house was passed to the legislature in August. In early September, it is expected that the government will arrange a date for a parliamentary debate which will probably take place in October. As the upper house may either accept the bill (the same one analysed in PL&B 'May 87 p.18) or reject it, the government has to be prepared to adopt a procedure to avoid starting the parliamentary process all over again. If necessary, the government would introduce an amending bill in the lower house dealing only with the additional points raised in the upper house. Currently, it is expected that the main bill will be enacted in October and start coming into force in the first half of 1989.

Mr. Peter Hustinx, Legal Advisor on Public Law at the Netherlands Ministry of Justice, will describe the bill and its impact on company operations at our conference in London on October 19th.

Switzerland: Dr. P. Muller, Head of the Data Protection Service at Switzerland's Federal Department of Justice, will speak at our October 19th conference in London on the Swiss Data Protection bill (see PL&B May 1988 pp.10,11). He will include the most important issues for companies such as its coverage of manual records and legal persons; rules for the export of name-linked data; relationship with company and labour law, and how the law will be enforced.