

## DATA PROTECTION NEWS FROM AROUND THE WORLD

### 1. International organizations

**11th International Conference of Data Protection Commissioners:** This year's conference was held in Berlin from August 29th to August 31st with particular emphasis on International Transfers of Personal Data. The final resolution (see page 19) managed to reconcile the need for free-flow of data with safeguards for protecting personal privacy.

The conference, hosted jointly by Federal Data Protection Commissioner Dr Alfred Einwag and Berlin Commissioner Dr Hans-Joachim Kerkau was held in the former Reichstag building situated next to the Berlin Wall. Dr Kerkau explained that the location of the conference at this venue symbolised Berlin's present day role as a bridge between East and West. With some 120 participants, the conference was the largest ever held. There were some notable first appearances - Japan and Hungary made their debut as did the new Privacy Commissioners from Australia and The Netherlands. Also present were Commissioners from the German Lander who are responsible for enforcing Germany's Data Protection Law in the private sector. The main meeting was preceded by a meeting of the Data Protection Commissioners new media working group on August 28th which drew up a resolution on telecommunications (see page 21).

A summary of the reports from the International organizations and participating countries follows. Next year's conference will be held in Paris September 19-21st and will focus on health data and data protection aspects of medical research.

**United Nations:** The UN commission on Human Rights (Sub-Commission on Prevention of Discrimination and Protection of Minorities) has prepared guidelines concerning computerized personal data files, drafted by Louis Joinet from France. They are expected to be passed to the General Assembly in late October. They include principles similar to the Council of Europe Convention and OECD Guidelines and indicate to UN members the minimum standards needed for legislation. Canadian Privacy Commissioner John Grace said that the Data Protection Commissioners should give the UN guidelines their blessing as a broad statement of principles. However, he observed:

- \* Several national Data Protection Authorities had not been invited to comment on the Draft Guidelines, for example, Finland and France. Indeed, there was no response at all from the governments of Norway, Denmark, Austria or the UK.
- \* There was no guarantee that the principles of the guidelines would be enforced, even if the General Assembly adopts them.
- \* The principles do not define privacy. However, they do include manual and automated data, fairness, accuracy, purpose-specification, access, non-discrimination, security, supervision and penalties, transborder data flows, and public and private sectors.

- \* There are broad exceptions, for example on public health. The guidelines are silent on the issue of data destruction where it would be useful to have a policy consistent with the collection and storage of archives for historical research.

The text is available from Privacy Laws & Business.

## **2. Countries with data protection laws**

**Australia:** The Federal Minister for Consumer Affairs, Senator Nick Bolkus, has now submitted to the Federal Parliament an amendment to the Privacy Act to extend the Privacy Commissioner's jurisdiction to credit information, which would be a major increase in his powers (see page 13). He is also monitoring privacy aspects of direct marketing and management-employee relations.

**Austria:** From now on, companies in Austria may sell lists to other organizations only with the informed and express consent of consumers. This decision taken earlier this year by Austria's Data Protection Commission probably reflects the worst fears of the European direct marketing industry. What is the reason for the Austrian decision and will this be a precedent for the rest of Europe?

The Austrian decision was the result of a case involving the Austrian direct marketing subsidiary of Bertelsman, the major German-owned advertising and publishing company. From the industry viewpoint, the case was intended to clarify how Austria's Data Protection Act should be interpreted. The Data Protection Commission decided to base its decision on a strict interpretation of the Austrian law, the Council of Europe Convention on Data Protection and its Recommendation on Direct Marketing (Precision Marketing July 31st 1989 p. 18). The legal argument focussed on how to interpret the principle that data should be stored for specified and legitimate purposes and not be used in a way incompatible with those purposes.

Although the company has appealed against this decision to the Supreme Administrative Court, it will take about a year for the case to be heard. In any case, this court cannot reverse the Commission's binding decision. It can only make the Commission reconsider the case on legal grounds.

(The Deputy Director of Austria's Data Protection Commission, Dr. Christian Singer, will explain this case, as part of the Direct Marketing session (which includes Data Protection Authority and industry speakers from Sweden, the USA and the UK) at the **Privacy Laws & Business Conference, "Managing International Data Protection in the 1990's"**, October 30-31st, Oakley Court, Windsor, UK. The session will include a discussion on whether the Austrian decision would be followed by other European Data Protection Authorities, and if so, when).

**Belgium:** Minister of Justice, Melchior Wathelet, has announced that he expects a new data protection bill to be published in a few weeks. This was the clear message from a seminar held on September 20th in Brussels. The

event celebrated the fifth anniversary of the Commission Consultative de la Protection de la Vie Privée, which has jurisdiction restricted to the use of the National Register, for example, national identity numbers. The new bill would be based on the 1983 bill (PL&B February '87 p.15) but would cover manual records and data held on personal computers. The police and security services would be subject to the law and supervised by a control body nominated by the legislature. The minister is currently considering its staffing and budgetary resources. The government's aim is that Belgium should be able to ratify the Council of Europe Convention.

At the same seminar, the Minister of Economic Affairs, Willy Claes, announced that the government was preparing regulations on the protection of personal data in the area of consumer credit.

**Finland:** Requests for exceptional permission for companies to use name-linked data in ways beyond those permitted by the Data Protection Act have mostly been refused by the Data Protection Board. In 1988, the Data Protection Ombudsman's office was mainly concerned with informing computer users and individuals of their obligations and their rights under the law (PL&B August '88 pp. 4-6). Early this year, Rita Wallin, the Ombudsman, launched a national information campaign by way of leaflets available through post offices and TV advertising. This publicity has led to much more use of the appeal mechanism in which companies can appeal to the Data Protection Board against a decision of the Ombudsman. So far, the Board has given decisions on forty-nine cases. The following are examples of appeals turned down:

- 1) The publishing of tax information on certain individuals
- 2) Direct marketing companies wished to store and use information about families' possessions; keep data on the clubs to which people belong; and keep data on how many children they have.

This year, the Data Protection Ombudsman (DPO) has appealed against decisions of the Data Protection Board to the Supreme Administrative Court in the following cases:

- 1) The Board gave permission for employers to gain access to job applicants' criminal records.
- 2) The Board approved the transfer of the tax collector's list of the amount of tax paid by individuals to the communes (local government authorities). The communes wanted this information to ensure that the payment of social benefits was more efficiently administered. However, the Ombudsman argued that the data was only really needed for dealing with particular cases. To collect such data on everyone would mean that the data would be irrelevant in most cases.

The Data Protection Board consists of seven people with legal and/or data processing experience nominated by the government for three years. It currently has: a law professor, a legal adviser to the local authorities association, a representative of the consumers association, a director of an

insurance company, a representative of the Chamber of Commerce and two representatives from the Ministry of Finance. The Board meets every two weeks, and has a full time secretary, Leena Sateri, who prepares the cases for the Board's consideration.

The most important categories of complaints to the Ombudsman are those about errors in credit files, identity number use, public health files and direct marketing. The DPO planned to begin inspection visits in September.

### Germany: Telecommunications

On 1st July this year the law concerning the restructuring of the post, telecommunications and Deutsche Bundespost came into force. Under the law, the Bundespost has been split up into the Federal Ministry for Post and Telecommunications, and the three public enterprises Deutsche Bundespost Postdienst (postal services), Deutsche Bundespost Postbank (postal banking) and the Deutsche Bundespost Telekom (telecommunications). In addition, telecommunication services, such as mobile phones, have been opened to private sector bidders. However, the Federal Government's draft law did not contain sufficient data protection rules. As a result of intervention by the Federal Data Protection Commissioner, Dr Alfred Einwag, the law now binds the Government to issue such rules. A point which has still to be resolved is who is the competent Data Protection Authority to enforce the law regarding those services run by private companies. The Bundespost itself will continue to be supervised by the Federal Data Protection Commissioner. An amendment to the Telecommunication Installations Act now clearly states that "anybody operating, monitoring, servicing or otherwise employed in operating telecommunications facilities designed for public communication, must keep telecommunications data secret".

### Health Care

The Federal Data Protection Commissioner, has managed to strengthen data protection provisions in the Health Care Reform Act to prevent the advent of the "transparent patient," the linking of separate health files into one database.

- 1) Only spot checks may be used to control economic efficiency. These spot checks involve 2% of doctors every three months. There is no direct link between the efficiency checks and the names of insured people, and there is no transfer of diagnostic data on electronic data media.
- 2) Storage of data in files is permitted for only short periods.
- 3) Research projects may be carried out only with data which has been made anonymous.
- 4) The use of people's personal numbers for the pension insurance fund will be illegal, from 1 January 1992.

### Genome (Genetic Code) Policy

The Conference of Federal and Lander Data Protection Commissioners has set up a working group to prepare a policy assessment for several areas involving chromosomes and DNA (PL&B May '89 p. 26). The group is focussing its attention on:

- 1) Legal proceedings
- 2) Employees
- 3) Insurance
- 4) Genetic questions in the health area, such as pre-natal diagnostics and the screening of new-born babies

**Iceland:** A new data protection law is due to come into force from January 1st 1990 on the expiry of the current law, reports Jan Thors, Secretary to the Data Protection Commission. Iceland is unique in having data protection legislation which has fixed terms. The first and second laws had terms of 4 years. The advantage of this procedure is that Iceland has a systematic and regular way of keeping up with changes in international legal and computer practice. A bill to introduce some minor changes into the law is currently before the Icelandic parliament. They include some provision concerned with direct marketing:

1. To require organizations who wish to use personal data for direct marketing purposes to obtain a special license; and
2. To make it clear to recipients of direct marketing communications the source from which their name was obtained.

In addition to the law undergoing review, the term of office of the present Data Protection Commission also expires at the end of the year. No decision has yet been taken on whether the present members will have their terms of office renewed.

**Isle of Man:** Registrations totalled 556 by the end of August, some 100 more than when the deadline was reached on April 17th this year. The Data Protection Registrar, Dr. Malcolm Norris and his staff, have started investigating the reasons for firms not completing the forms. He considers that the total number of registrations should exceed 1,000. The most common reasons given for not registering are companies' claims, usually incorrect, that they are covered by one of the narrow exemptions, while others claim that they have not had time to take action.

He has also started handling complaints, although he does not have his full supervisory powers until 17th October 1990. However, Dr. Norris finds that he receives co-operation in investigating complaints due to the fact that he operates in a small community where local radio and newspapers provide ideal media for public discussion of the issues. By the end of August he had received 21 complaints, of which nearly half were concerned with credit information. The Registrar's first annual report is due to be published on 17th October this year.

### British Isles Data Protection Co-ordination Group:

On 27 September, there was a meeting in The Isle of Man of the heads of the Data Protection Authorities from Guernsey, Republic of Ireland, Isle of Man, Jersey and the UK, in the second of their six monthly meetings. They discussed:

- 1) Their different approaches to the registration process.
- 2) The major issues facing them, like credit information.
- 3) How their laws cover the processing of name-linked data outside their jurisdiction - some aspects are not clear, such as the need for companies with headquarters in the UK to register branches in the offshore islands.
- 4) The UK Registrar's review of the Data Protection Act and his recommendations for its amendment.
- 5) The resolutions passed by the Berlin International Data Protection Commissioner's Conference (see page 19).
- 6) Improving cross-border communications within the region such as procedures for handling complaints.
- 7) Access to medical data - the British Medical Association is preparing a code on confidentiality.
- 8) The communication of examination results - since Ireland's Data Protection Act was passed, the Irish Universities have adopted a new policy of communicating results direct to students and not through their educational establishments.
- 9) The different approaches to credit information policy.
- 10) The appeal to the UK's Data Protection Tribunal by The Halifax Building Society (the UK's largest home loan institution) and its prosecution in the magistrates court for not fully registering the purposes for which its data is stored. The appeal hearing has subsequently been postponed until the court action has been completed.
- 11) Police data - employers sometimes request a check on a job applicant's police record. There is a plan by the Isle of Man police to require the employer to indemnify them against liability in case they release incorrect data.
- 12) Organisations relying on narrowly defined exceptions in order not to register. For example, agents in The Isle of Man of an international consumer service wrongly claimed that their system came within the accounts exemption - their terminals were used both for accounts and for order processing

- 13) Pension Funds provide a good example of Transborder Data Flows and national jurisdiction - where a pension fund involves trustees, a management company and an insurance company in two or three different jurisdictions, who is the data user and where should he register?

**Israel:** Sarah Barsela was appointed to the post of Registrar of Data Bases from 1st January this year (see p.26). She was formerly head of the Ministry of Justice's Legal Aid Division. She informs PL&B that there are plans to amend Israel's Data Protection Act next year with particular emphasis on the definition of personal data and data base.

**Jersey:** The cost of registration has increased from £20 to £50 per register entry this year. The total number of entries made in the Register has now reached 700, of which 45% relate to the banks and finance companies. The maximum fee payable by data subjects to obtain access to their files remains at £5 per enquiry. Since the law was passed, regulations have provided subject access exemptions to health and social work data, and data held by financial regulatory bodies.

**Luxembourg:** The Data Protection Commission's term of office is due to expire in January 1990. In the course of the last eighteen months, at the request of the Minister of Justice, the Commission has begun to consider some amendments to Luxembourg's Data Protection Legislation which came into force on 31st March 1979. The following points are receiving priority:

- 1) The scope of the law
- 2) The way the law applies to the private sector
- 3) Transborder data flows
- 4) The principle of "equivalent security"
- 5) The powers and methods of the Commission

During the last year, the Commission persuaded the government to accept its view on the need for restrictions on the linking of income tax and social security files.

**The Netherlands:** The President of the Netherlands Data Protection Registration Chamber, K. de Vries, has established his office (see page 27) and is now hiring staff. He has started discussions with trade associations on their codes of conduct.

The Netherlands Direct Marketing Association has prepared a draft of its code of conduct and is now discussing it with the Consumers Association. The plan is to finish these discussions by the end of the year and then submit it to the Registration Chamber for its approval (PL&B November '88 p. 14).

**Sweden:** The Data Inspectorate's new Director General is Ms Stina Wahlstrom, formerly a top civil servant at the Ministry of Labour.

The Data Inspectorate is increasingly working on general regulations, advice and guidelines as well as information to the public. These include:

- 1) Regulations and recommendations on debt collecting
- 2) Regulations concerning personal files for statistical purposes
- 3) Guidelines on blacklists
- 4) Guidelines on files for company health care

**United Kingdom:** Eric Howe, the UK's first Data Protection Registrar, has had his term of office renewed for another five years, the Home Office announced on 20th September. The decision comes at a turning point in the Registrar's activities. In the last year, his office has taken formal enforcement action against both private and public sector organizations which have breached the Act, and he has made several recommendations for radically amending the Act after a year's review. The Act is simultaneously under review by an inter-departmental government committee which has been requested by industry representatives to make the Act less burdensome.

Enforcement Notices: The Registrar's fifth annual report, published on 12th July, for the first time names companies against which he has served Enforcement Notices (PL&B May '89 p. 10). They are: Chartsearch PLC, the Halifax Building Society, Sharps Individual Bedrooms Ltd, and the Church of Scientology College of Religious Education Inc.

All these organizations agreed to comply with the Registrar's requirements, except for the Halifax Building Society which has appealed against its Enforcement Notice on the extent of the right of access to the Data Protection Tribunal. Although the hearing was set to begin on October 10, it was postponed when the Halifax Building Society was simultaneously prosecuted by the Registrar for "knowingly and recklessly:" holding data for an unregistered purpose; for disclosing data to a person not registered; and obtaining data from a source not registered. The Magistrates' Court in Halifax, the town where the Building Society's Headquarters are located, is due to hold its formal first hearing on October 16th this year.

Complaints: The total number of complaints received by the Registrar's office in the year ended 31st May was 1,122, compared with 836 in the previous year. Approximately 35% of all complaints were on consumer credit, with about 16% on direct mail, and 18% on subject access. In addition to these complaints, some 30,000 telephone enquiries were dealt with over the year.

Enforcement in the public sector: In June and July, the Registrar intervened to prevent the collection of irrelevant personal data by local authorities in their preparation for the collection of a new tax, the Community Charge. This received considerable public and media attention. On 22nd June, he upheld a complaint that the collection of information by the



Trafford Community Charge Registration Officer was in breach of the Data Protection Principles. The legal issues were in brief:

1. Was the information fairly obtained?
2. Was the information excessive for the purpose of the collection?

Mr Howe required the Trafford Registration Officer to delete the information he held on computer about the relationships of people in households and to cease issuing the forms which were the subject of the complaint. The Registration Officer also promised to issue new forms which collected the necessary information fairly, and not to release to his Borough Council manually held information to which the Mr Howe objected. This case led his office to carry out a survey of all the Community Charge forms in England and Wales and found that over 20 had asked the same question on relationships as Trafford. By contrast, in Scotland, the situation was simplified by using an identical registration form throughout the country.

Registrar's Review of the Data Protection Act: The Registrar's wide-ranging review occupies over 50 pages of his annual report. The main themes with an impact on the private sector are that:

1. The principles attached to the Act are broadly right and should be followed by all computer users.
2. The registration process should be simplified because it is too complex.

Most users have focussed on the registration issue. The Registrar considers that some form of registration is useful because: it enables his office, as the enforcement authority, to know the location of personal data users, and encourage and, if necessary, force them to comply with the law; it is helpful to the people who register because it gives them a reference point to guide them to the law's requirements; and it raises revenue which helps promote the independence of the Registrar's office.

The Registrar has recommended a limited registration scheme which would reduce the number of registrations from some 180,000 to an estimated 50,000 data users which process sensitive data. Under this plan, financial institutions, credit information and direct marketing companies would need to register, but many small businesses which do not process sensitive data would not. Under such a plan, Mr Howe would need stronger enforcement powers.

Codes of Practice: His attitude towards the Act is that "it should aim to be prescriptive, that is, it should not tell people how to do things." The law must remain flexible and as a result, he does not recommend statutory codes of practice, although they could function with a status similar to the Highway Code. For example, they could play a useful role in providing guidance to the Data Protection Tribunal.

Strengthen powers of the individual: At present, only data users may appeal to the Tribunal against the Registrar's Enforcement Notices. Mr Howe considers that individuals should also be able to appeal against his decision. In effect, this would mean that an individual would be asking the Tribunal to issue an Enforcement Notice.

### 3. Countries planning data protection laws/rules

**Hungary:** The government is preparing to approve a Data Protection Bill which will be based upon and consistent with the Council of Europe Convention and is proposing to sign, and in due course, ratify that Convention. Work on this subject has been based at the Central Statistical Office which is Hungary's centre of expertise and policy both on computer technology and also related legal issues. Dr Pal Konyves-Toth of the Central Statistical Office explained the background of the bill to the Berlin Conference. Hungary was the first of the Eastern European Communist countries to publish official computer statistics, a decree on software copyright and a decree on the protection of computer equipment against fire.

The right to privacy derives both from the Constitution and the "International Convention on Civil and Political Rights" which was announced by a decree of the Presidential Council in 1976. Then in 1984, the President of the Council of Ministers gave his approval for the Central Statistical Office to study data protection. As a result, when political developments became more favourable last year, the CSO was prepared with a set of data protection principles and the first draft of a bill, mainly put together by Professor Solyom. This work was integrated into the reform of Hungary's political institutions. In January this year, the President of the CSO and the Minister of Justice submitted the draft of a combined Data Protection and Freedom of Information bill to the Council of Ministers. The Council approved it immediately, and made time for its enactment in due course.

A new Constitution is currently being prepared containing the following clause: "The Constitution has to recognize every human being's right to the protection of personal data." It further states that: "The Constitutional provision on liberties has to acknowledge everybody's right of access to information of public interest." These Constitutional provisions will be regulated by law.

Hungary's ties with the international legal community have been strengthened by it having been granted special observer status at the Parliamentary Assembly of the Council of Europe, and in the participation of its Justice Minister in June at the conference in the Hague of the Council of Europe's Ministers of Justice.

**Portugal:** A new version of the Constitution was enacted on 8th August this year, with a new article 35 on Data Protection and Transborder Data Flows (see page 18). A revised Data Protection Bill is being prepared. (PL&B February '87 page 20).

**Switzerland:** Switzerland will have a data protection Act by 1992 at the earliest. The Swiss Data Protection Bill (PL&B May '89 page 12) is currently being discussed at the first parliamentary stage in a committee of the Conseil des Etats, which represents the cantons, and is expected to be adopted in the course of this winter or next spring. This will be followed by discussion of some two years in the Conseil National, which is directly elected.

The following changes are envisaged:

- 1) The powers of the data protection authority will be limited in the private sector. It would have the function of an ombudsman and would no longer have power to bring cases to the attention of the court.
- 2) Sensitive data is no longer listed in detail in the law, but described in a general sense. As a result, sensitive data is that which poses a particular risk of infringing an individual's privacy on grounds of its significance, method of processing, or relationship with other data. For example, data on political opinions, health, race or sexual habits, may be sensitive data but it is a question of deciding in each case if it is truly sensitive.
- 3) Private sector users of data are required to register their files with the data protection authority only if they regularly process sensitive data or personality profiles, which are not yet defined.
- 4) The processing of data which has been made accessible to all by the data owner (for example, a publication), has been made easier.

All these examples show that so far, the trend in these parliamentary discussions is towards a weakening of legal requirements for data protection in the private sector. By contrast, in the public sector, few modifications of the bill have been discussed.