PRIVACY LAWS & BUSINESS

Publisher: Stewart H Dresner **Editor: Merrill Dresner**

No.1 **February 1987**

Welcome to the first edition of Privacy Laws and Business, as far as we know, the only European newsletter devoted wholly to helping companies to monitor the impact of privacy or data protection laws on company operations.

Some readers may be called data protection managers, although many will combine that role with another management function. But everyone responsible for data protection policy in their company has the delicate task of understanding the implications of the national data protection laws and bills - and the international provisions - and implementing them.The main areas of corporate impact are personnel files, management-labor relations, marketing lists, data exports and the introduction of office automation. Privacy Laws and Business will cover all these areas.

In the April issue we shall look at the export of name-linked data.This feature will include a comparison of the OECD Guidelines with the Council of Europe Convention, and an assessment of the new Austrian rules compared with those of countries which have ratified the Council of Europe Convention. Perhaps you would like to raise some questions, if necessary in confidence, arising from your own experience of dealing with data protection authorities, indicating some areas where you have had problems or see them coming.

You will get maximum value from your subscription if you use Privacy Laws and Business as a forum for sharing your data protection experience with other companies in what is for everyone a non-competitive area.

We look forward to keeping you well informed on data protection issues.

Stewart Dresner, Publisher

Merrill Dresner, Editor

In this issue

Publisher: Stewart Dresner, 3, Central Avenue, Pinner, Middlesex, HA5 5BT, United Kingdom, (+44.1) 866 8641.

DATA PROTECTION NEWS FROM AROUND THE WORLD

The data protection scene is ever-changing. On the international front, the Council of Europe Convention is developing from its original status as a legal instrument covering broad data protection principles. The Council of Europe is now also acting as an umbrella for recommendations which apply the Convention's principles to a wide range of sectors. On the national scene, after a few years, existing laws are amended and administrative or court decisions clarify how the legislation is interpreted in practice. Meanwhile, other countries move slowly toward passing their own data protection legislation, each with its own characteristics.

The Council of Europe

Last year, Cyprus and the Republic of Ireland signed the Council of Europe Convention (for the Protection of Individuals with regard to Automatic Processing of Personal Data), indicating their firm intention to introduce a data protection law. This brings to 16 the number of countries which have now signed the Convention. The others are Austria, Belgium, Denmark, France, the Federal Republic of Germany, Greece, Iceland, Luxembourg, Norway, Portugal, Spain, Sweden, Turkey and the UK. The only EEC countries to have not signed so far are Italy and the Netherlands, although both governments intend to sign when they are closer to passing data protection legislation.

This year, it is expected that Austria, Denmark, Luxembourg and the UK will ratify the Convention, joining France, Germany, Norway, Spain and Sweden which have already done so.

Mr. Hustinx of the Netherlands Ministry of Justice is the new chairman of the committee of data protection experts, replacing Professor Spiro Simitis, the data protection commissioner of Hesse, Germany.

Several working parties are drafting recommendations which will apply the principles of the Convention to specific sectors. The most important for business so far, is the recommendation on direct marketing, adopted in October 1985, (the text and a reprint of my 3 page report on the recommendation are available on request).

The working party on employment, chaired by Vito Librando of Italy's Justice Ministry, is preparing a draft on applying the principles of the Convention to employee related issues. They include: the collection and use of employee data (raising the issue of employees' collective as opposed to individual employee rights; the monitoring of employees by audio-visual techniques; telephone logging; and genetic screening (used, for example, in the nuclear industry to assess an individual's risk of contracting cancer by

examining an individual's family history). The recommendation will be adopted by the end of 1987 at the earliest. There will be a major feature on the impact of data protection laws on management-labor relations and the union response in the July issue of Privacy Laws and Business.

The working party on new technology, chaired by Manuel Herredero, a senior member of Spain's data protection government team, is covering data protection aspects of: telemetry, the automated remote collection of data like household or industrial energy consumption; electronic mail; and interactive media like teleshopping. The working party has sent a questionnaire to member states and its third meeting will be in March.

A working party on the banking sector will meet for the first time in June to discuss data protection aspects of issues like smart cards and electronic payment at the point of sale. A working party on the collection of data is aiming to produce a final document by the end of 1987.

Countries with data protection laws

Austria: In July, the 1978 data protection act was amended and the new provisions covering rules for the export of name-linked data were approved -- to come into force from July this year. See the April issue of Privacy Laws and Business for further details.

Denmark: A bill amending the data protection legislation was published late last year following a conference organized by the Justice Minister in the spring. The conference recognized that developments since the legislation was adopted in 1978 meant that there was now an increased wish for greater self-determination or control over the data by individuals, and a wish for more openness in both the private and public sectors.

The first step was the introduction of a regulation in September limiting the type of information recruitment agencies may legally collect, store and disseminate.

Shortly afterwards, a bill amending the data protection legislation was introduced by the Justice Minister into the parliament. The bill was circulated to interested organizations for comment and their responses are due to be received by mid-January. Is is expected that there will be a full debate in the parliament and that the amendments will be passed this spring.

The main points in the draft amendments are:

1. The introduction of a general right of access by data subjects to name-linked data on them in the private sector. The Data Surveillance Authority (DSA), from last year headed by Bent Ove Jespersen, has wanted this provision for many years, as it

would enable Denmark to ratify the Council of Europe Convention.

2. A registration of automated files containing sensitive data in the private sector. Such files would require the permission of he DSA to ensure that data on individuals is kept to an essential minimum. However, the DSA points out that a mass registration of sensitive files, as in Sweden, France and the UK, would be expensive. If organizations merely informed the DSA that they collected, processed, held and transferred sensitive data to other persons, there would be no evaluation of the files or organization and no increase in the level of data protection. Such a system would offer the appearance of data protection without the substance.

3. Restrictions on selling customer lists for direct mail purposes.

4. Restrictions on credit information bureaux regarding the type of consumer information they may collect and transfer to other parties.

5. Including private sector research within the scope of the data protection legislation.

Germany: The government has submitted an amendment bill to the Bundestag that would:

1. Strengthen the principle that data should be used only for a specific purpose. This would bring the data protection act into line with the Federal Supreme Constitutional Court census case decision in December 1983.

The court stated that that the protection of the individual against unlimited collection, storage, and communication of his personal data is covered by the general right to privacy given by Germany's Basic Law. This basic right ensures that the individual can himself determine the disclosure and use of data on himself. A restriction to this general right is admissable only in the prevailing interest of the general public. A company wishing to computerize its worker productivity, attendance, and disciplinary records against the wish of its work force would not necessarily be considered by a court as representing such a prevailing interest. (See page x on how these principles were applied in the Opel v. IG Metall case).

2. Strengthen the rights of an individual to gain access to information on himself.

3. Grant recourse to individuals to claim damages if illegal use is made of automated name-linked data.

4. Strengthen the powers of the Federal Commissioner for Data Protection, although the Commissioner himself, Dr. Reinhold

Baumann, considers that in some instances his powers would be weakened.

The SPD party submitted its own amendment bill in 1984 and others have submitted amendment bills also. Assuming that none of these bills are passed by the time of the general election on January 25, they are likely to move back onto the agenda in the new parliamentary session.

Sweden: The Swedish Data Inspection Board (DIB) headed by its new Director-General, Mats Borjesson, in September launched a major publicity drive to increase registrations in the private sector. The DIB sent letters to every company with more than one employee, 120,000 in all. By the end of December, nearly 7000 new applications had been registered making a total of 25,000 licences. The number of files held by each "responsible keeper" is not a deterrent to registration as the annual license fee of Skr.240 pays for as many files as the "responsible keeper" wishes to register. In addition, the DIB gives permission for organizations to use some 2,000 files containing sensitive data or data for export.

In 1987, the DIB will increase its inspection programme and is recruiting two data processing specialists to help the existing DIB personnel who divide their time between registration, enforcement and inspection duties. By the end of 1986, it had not yet been decided whether the inspection programme should concentrate on specific sectors, like direct marketing, or on how the law is being implemented.

The United Kingdom: The Data Protection Registrar, Eric Howe, announced last month that having now registered all outstanding applications, his investigation department is now matching the register entries against published lists to identify data users who have not registered. He is investigating both private and public sectors including finance and direct marketing organizations. Howe warns,

"I shall be writing to organizations who we are unable to trace on the register, but whom we suspect may be holding personal information about individuals on their computer systems. The object is to sweep up as many malingerers before 11 November, 1987 when individuals will be able to exercise their right to see personal data about themselves held on computer."

"Our primary task is to protect the interests of the public and, as time passes, we shall take an increasingly serious view where we believe that data users have been lax about their responsibilities and especially so where there is evidence that they are deliberately flouting the law." Companies which have not registered face the penalty of unlimited fines in the higher courts.

If any readers are at companies which have automated name-linked files but have not registered, Data Protection Registration Packs are available from Crown post offices (those that do not share premises with another business). From May 11, 1986, the holding of personal data or acting as a computer bureau by an unregistered person has been a criminal offence. Registered data users must operate within the terms of their register entries. Data users from this date have been liable to pay compensation as a result of damage or associated distress caused by inaccurate personal data. A court may order rectification/erasure of inaccurate personal data.

From November 11, this year, data subjects will have a right of access to data on themselves. The Registrar will then be able to use his full supervisory powers. Any notices, such as forbidding data exports or shutting down data processing operations, which he may have served before this date, will now come into effect.

The best organized companies have now arranged who will be responsible for: monitoring compliance with the data protection principles; warning of changes necessary in your company's registration entry; and answering data subjects' access requests and complaints before they have their rights under the law. Now is an ideal time to give your data protection procedures a test run before the Registrar has formal powers to deal with complaints.

He has already received over 160 complaints and has declared that he will provide an effective ombudsman service to deal with grievances. This year, companies can expect data subjects like employees, customers and suppliers to become more aware of their rights as the Registrar publicizes them through a media campaign in the period leading up to November 11. Companies should realize that there will inevitably be great publicity over his first complaints investigations and decisions.

Countries planning data protection laws/rules for companies

Belgium: The data protection bill is currently before the relevant parliamentary commission, which is expected to discuss it in the next few months (see page x).

Canada: The parliament's Standing Committee on Justice and Solicitor General held hearings from May 6th to June 19th last year to review the Access to Information Act and the Privacy Act after they had been in force for three years. The hearings on the Privacy Act included the issues of: exempt data banks; judicial review; computer matching; and the possibilty of extending it to Crown corporations and the private sector. Privacy Commissioner, John Grace, proposed that the government consults the Commmissioner when new laws with privacy implications are proposed, so that he would carry out in effect a "privacy impact study." This already occurs

on some occasions.

One of the major issues is the scope of the law - to what extent the Privacy Act should be extended to the private sector. Grace proposed extending the law to cover federally owned bodies, like the Canadian Broadcasting Corporation, Air Canada, the Canadian National Railway, and Petro-Canada. Some advocated extending the Privacy Act to federally regulated bodies like Canadian chartered banks telephone and cable television companies both sectors regulated by the Canadian Radio-Television and Telecommunications Commission but Grace did not argue for that postion. In fact, he makes it clear that it cannot be assumed that if the Privacy Act covered Air Canada it would also extend to private sector airlines. For example, the Act already covers the Canada Post Corporation but it does not extend to similar private companies like courier services.

However, Grace has argued in his annual report that the government should take active steps to encourage private companies to support and apply the OECD Guidelines (on the Protection of Privacy and Transborder Flows of Personal Data) to their organizations. Canada formally endorsed the Guidelines in June 1984. As a result, the government said it would undertake a programme, "to encourage private sector corporations to develop amd implement voluntary privacy protection codes," but so far it has not done so.

However, companies should not assume that the government will never take action to encourage private sector compliance. The reasons are:

1. The principles of data protection apply equally to the public and private sectors. These include not only the usual rights of access, correction and redress but also concern over computer matching. Grace explains that the Privacy Act forbids the use of personal information except when used "for the purpose for which the information was obtained...or for a use consistent with that purpose." Since computer matching involves the comparison of personal information collected for different purposes, the practice contravenes this provision of the Act.

The implications are clear. "Computer matching turns the traditional presumption of innocence into a presumption of guilt. In matching, even when there is no indication of wrong-doing, individuals are subject to high technology search and seizure. Once th principle of matching is accepted a social force of unyielding and pervasive magnitude is put in place."

2. There is growing public awareness of data protection principles. For example, more than 100,000 people have used the act in the last three years. Furthermore, complaints to the Privacy Commissioner have increased not because of an increase in abuses but because of a greater awareness of data protection

issues. The media has played a part by revealing, for example, the careless disposal by the Winnipeg Employment and Immigration office of personal data on individuals participating in employment assistance and industrial training programmes with the result that the documents were found in an alley behind the office.

3. Grace points out in his most recent annual report that it was anomalous that the Privacy Commissioner had no mandate to deal with privacy issues arising from electronic monitoring or surveillance in the workplace (note that the Council of Europe's employment working group is also dealing with this point).

4. There is a close working relationship between the public and private sectors and name-linked data does pass to the latter. When it does so, the public expects standards of data protection to be maintained. The media, for example, revealed that Employment and Immigration Canada contracted out a telephone and postal survey of unemployment insurance recipients to Peat Marwick & Associates. In doing so, it released the names of the individuals without informing the company of its consequent obligations under the Privacy Act, such as telling the individuals the purpose of the survey.

The timetable is that the parliamentary Justice committee is due to meet by the end of January to consider its report. It will be important to watch the government's response when it is published to see whether it is yet ready to honour the commitment to encouraging private sector compliance with the OECD guidelines, and if so, the form it will take, and the extent to which the Privacy Act will be extended.

Finland: The appropriate parliamentary committee held hearings on the data protection bill from September. No major changes are expected, and the bill should pass into law before the March election this year. There will be a full report in the April issue of Privacy Laws and Business.

Netherlands: A parliamentary committee gave its comments on data protection in April last year. Since then, the government has been preparing its response, which is due for publication this month. A public debate will take place over the following few months, and the Upper Chamber of parliament is expected to approve the bill in the second half of 1987. The law should come into effect in the first half of 1988. There will be a full report in the April issue of Privacy Laws and Business.

New Zealand: An academic consultant spent several months last year studying data protection laws covering the private sector in several countries on behalf of the government. He expects to present his paper to the government by the end of January. While the Justice Minister has made no prior commitment to an initiative in the data protection area, it is quite possible that an announcement of government intentions will be made this year.

However, given the present government's commitment to deregulation, a system of mass registration for corporate data users, as in the UK and France, is unlikely.

New Zealand already has an Official Information Act which came into force on July 1 1983. It groups together in the same law access to a person's government records on himself or herself and access (subject to certain exceptions) to official information, including the broad range of government records.

Portugal: Parliament will take a decision in February whether it will debate in the current session the data protection bill (see page y) prepared by the Ministry of Justice. If so, the debate is likely to take place in April or May.

Switzerland: The Data Protection Commission submitted a revised bill to the Ministry of Justice late last year. The minister is expected to publish the bill by mid-year, and this will be followed by discussions in parliament. The bill will cover natural and legal persons, manual and automated data. The new bill strengthens a worker's rights to data on himself and limits employers' freedom to collect and process certain name-linked data.

Full details of the bill have been held over but will be published in **Privacy Laws and Business** when the bill is published by the Minister of Justice.