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.

European Data Protection Laws

	Austria	Denmark	France	Germany	Iceland	Israel	Luxembourg	Norway	Sweden	U.K.
AUTOMATED	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
MANUAL		✓	✓	✓	✓			✓		
PHYSICAL	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
LEGAL	✓	✓			✓		✓	✓		
CORRECTION	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
APPEAL DATA AUTH	✓	✓	✓	✓	✓			✓	✓	✓
PENALTIES	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
COURTS	✓	✓	✓	✓		✓	✓	✓	✓	✓
EXPORT AUTH'S'N	✓	✓	✓		✓	✓	✓	✓	✓	✓

PRIVACY LAWS AND MANAGEMENT-LABOR RELATIONS

In all European countries with data protection laws, employees have the right of access to automated -- and in some countries, manual -- management files on themselves, and they have the right to correct them, or at least insert a statement of disagreement. As a result, managers are becoming more careful about what they write in reports when evaluating workers' performance. Certainly, managers are taking greater care to ensure that data is accurate.

In some firms, the coming into force of a data protection law has been the stimulus for a radical review of record-collection policy. Several companies have reduced the amount of data they collect to a necessary minimum. IBM, for example, has made the decision to reduce the scope of its employee records in all European countries: the company no longer asks employees their religion; and job applicants are no longer asked their age, marital status or next of kin.

IBM employees have the right of access to management evaluation of work performance, whether processed automatically or manually, as well as the right to add a statement of disagreement should they wish. However, employees are not given access to management assessments of an individual's future career prospects, as this could lead to misleading hopes and impressions.

Undoubtedly, some managers in companies operating in countries with a data protection law covering only automated records are tempted to take advantage of this by storing unfavorable comments and evaluations in a manual system. The company then has the problem of making reference to these comments -- e.g. if the employee record says, "See manual record for performance evaluation," this is certain to attract the interest of the data subject.

The evidence from around Europe is that fewer workers ask for access to their files than might be expected. Some companies charge an access fee while others do not, so cost should not be seen as a barrier to such requests.

In several countries, labor unions are actively intervening in data protection issues. For example, France's Commission Nationale de l'Informatique et des Libertes in its sixth annual report published last year, it lists the following subjects as those most frequently raised by French labor unions:

+ installation of company telephone logging systems;
+ change in purpose and use of management personnel files;
+ use of social security numbers in management files to identify people;

+ implementation of control systems using access badges to allow entry to certain company areas; and

+ entries in management personnel files showing, in particular, salary deductions.

The July issue of Privacy Laws and Business will have an in-depth feature on the impact of data protection laws on management-labor relations.

IG METALL vs GM'S ADAM OPEL: ROUND ONE TO THE COMPANY

Although there are more court cases over data protection issues in Germany than in the rest of Europe put together, last year's court decision in the IG Metall-Adam Opel case demonstrates the impact of data protection laws on management-labor relations Europewide.

The case centers on union opposition to Opel's transferring its data processing to a wholly owned subsidiary, Electronic Data Systems (EDS).

In its written decision, the Hesse state court in Darmstadt explained that it did not find violations of the German Federal Data Protection Law (BDSG) in Opel's turning over the automaker's data processing to a new GM subsidiary, EDS. EDS in Germany is a wholly owned subsidiary of Electronic Data Systems of Dallas, Texas, which was acquired by GM in 1984. EDS handles personnel data for Opel as well as functions such as CAD/CAM. In addition to other laws, Opel based its case on the fact that the company turned to EDS to improve its data processing in order to recover from serious losses in recent years.

The court's judgment covered six main points:

The works council retains its legal rights. The court rejected IG Metall's claim that in contracting out its data processing to EDS Opel had deprived its works council of its right to see that employees' personal data was properly protected. The court explained that the company remains answerable to the works council for the data because this responsibility does not end when data processing is turned over to a third party (Article 37, BDSG). When a firm turns over its data to a data processing firm, a contractual relationship exists between the two enterprises, and the company (in this case Opel) remains "responsible for the data." This means that Opel's works council may still exercise its lawful authority over EDS's processing of employees' personal data.

Individual employees retain their rights. In addition, each Opel employee retains his or her right of access and explanation concerning his or her personnel file, as provided in the Law on

the Constitution of Enterprises (BVG). This right is also guaranteed by the data protection law when data is administered by a third party.

The data processing firm is an authorized party. The court ruled that EDS could not be considered an unauthorized third party whose access to data is prohibited by Article 2, Paragraph 2, of the data law because EDS's right to the data is given through its mandate from Opel to process the data.

Illegal data exports are a risk but not a danger. Setting up an EDS subsidiary in Germany to handle Opel's data turned out to be a legally sound move (both are located in Russelsheim, near Frankfurt). The court rejected IG Metall's claim that Article 24 on transborder data transfer was violated. There was a "theoretical possibility" that individual items of data could be sent outside Germany, the court said. But supervising such incidents is part of the general question of supervising data storage, and the "theoretical possibility" is not an indication of a "concrete danger" that EDS would send Opel data illegally out of the country.

The data processing firm is qualified for the task. Opel's claim about EDS's qualifications was not contested by the union, the court noted, and it ruled that there were no grounds for maintaining that the auto firm had not exercised appropriate care in selecting an outside data processing firm (Article 8). For the same reason, the court added, there were no grounds for claiming that Opel had neglected its workers' interests in letting EDS store and process company data.

Violation of constitutional rights did not occur. IG Metall's contention that turning the data over to EDS had violated Opel workers' constitutional right to information also got nowhere. That could not apply to a legally made contract, the court decided.

IG Metall has announced that it will appeal against the court's decision.

DATA PROTECTION MANAGEMENT CHECKLIST

Data protection laws give rights to individuals on whom data records are kept to gain access to those records and correct them if they are wrong. Companies should now make sure that they are prepared for the tensions that could develop when employees read managers' evaluations of their performances.

To help minimize potential problems, companies should appoint a manager who is responsible for complying with data protection legislation. He should ensure that he knows:

+ where the company's name-linked files are kept;

+ who manages them and is responsible for training staff on data security procedures;

+ whether there is a companywide policy on how frequently to review records to ensure they are up to date;

+ whether there is an agreed maximum period before records are destroyed;

+ whether name-linked files are registered with the appropriate authorities in each country where this is necessary;

+ whether the company's export of data complies with national law and has the appropriate national approval;

+ whether by complying with US law on monitoring the employment of minority ethnic groups the company data files will conflict with any European national laws on compiling sensitive data on racial or ethnic groups.

PRIVACY LAWS AND FINANCIAL INFORMATION

The introduction of data protection legislation will affect two main areas of financial information:

+ data on individuals' bank accounts, insurance policies etc.,

+ data on individuals' credit worthiness.

In the first case, the individual knows that he has a bank account or an insurance policy and which financial institution he deals with. He has a contractural relationship and if he wishes to seek access to his record to exercise his data protection rights, he knows where he must make his request.

The second case is quite different in data protection terms because in this instance the individual data subject does not normally have a contractural relationship with the data owner. The credit information company can collect information on an individual and supply it to a third party without the data subject being aware of the process. The data subject may be aware of the data collection process only when he seeks and is refused credit or is granted credit at unfavorable terms.

For this reason credit information has been regulated by separate laws in some countries, for example, Sweden and the UK. Indeed in the UK, the Consumer Credit Act of 1974, giving individuals a right of access to their credit information records, was passed a

decade before the Data Protection Act in 1984.

Examples of the impact of data protection laws on credit information operations may be drawn from across Europe:

+ Complaints. In several countries, such as Denmark and the UK, the second highest category of complaints to data protection authorities, after direct marketing, concerns credit information. In the UK Data Protection Registrar's second annual report published in July this year, he states that the problem is the relevance of information held to provide credit references. "Broadly, the concern is about the supply of information not apparently directly related to the individual requesting credit."

+ Investigations. The volume of complaints often leads to the data authority making a special study of this sector. One chapter of the recently published annual report from France's data protection authority reported on its work in this area.

+ Registration. If a country has a detailed and simplified data protection registration form, like France, credit information comes into the detailed category.

+ Licensing. If a country, like Denmark, has a data protection licensing system for certain categories of business, then credit information bureaus will be included.

+ Shutting down an operation. Among the few examples from around Europe where a company has had its operation shut down is a credit information company in Norway.

+ Exporting name-linked data. In Germany, The Land (provincial) officials responsible for enforcing data protection legislation for companies meet three or four times a year to discuss common problems so they can implement consistent policies. On one occasion, they discussed how the German law should be applied to the export of credit information.

Their starting point was that the export of credit information from Germany is illegal if a domestic transfer would be under the same circumstances, or if there is a clear lack of data protection in the country receiving the data. They then considered whether credit information should be exported to an inquiry office in Austria, which does have a comprehensive data protection law. The owner of the data in this case was SCHUFA, the Protective Association for General Credit Precautions. It has a data bank on about 21 million people and stores information on individuals' loans, methods of repayment and, for example, whether the repayment schedule has been met. The Land officials took the decision to permit data to be sent to an inquiry office in Austria that accepted requests for individuals' data stored in Germany. Although an inquiry about an individual was allowed, it would not be permitted to answer a request for the creditworthiness of a large group.

AN OVERVIEW OF THE BELGIAN DATA-PROTECTION BILL

The first data-privacy bill was submitted to the Belgian legislature in 1976 and was followed by some other drafts, none of which reached the legislature. The current bill is based on one dated Nov. 10, 1983, and there is a reasonable prospect that it will pass into law in 1987. The only change from the 1983 bill is that Chapter I of that version, which made it an offence to watch, listen or record a private conversation, or any other type of private communication, without permission, has now been put into a separate bill.

Timetable

Sponsored by Justice Minister Jean Gol, the current draft legislation was presented to the legislature's lower house on Nov. 10, 1983 and has received detailed study by the Council of State. Its next step, scheduled for the parliamentary session beginning October 1986, will be further scrutiny in the lower house by the Justice Committee, followed by a full debate and then the same process in the upper chamber. The bill will then be either adopted or returned to the lower chamber. This process could take several months, but companies or trade associations wishing to influence the debate should contact friendly members of the legislature without delay. When the bill is passed, this year or next, it is likely that there will be an interval of two years before it comes into force. Companies will have much to do to prepare themselves before that happens.

Scope

The bill has been drafted to conform with the Council of Europe Convention, which Belgium signed on May 7, 1982. The new legislation will give rights to physical persons and will cover automated data processing of a personal character in both public and private sectors. Automated processing is defined in Chapter I of the bill as wholly or partly automated operations for the recording, storage, modification, erasure, selection or transmission of data. Data of a personal character is defined as data on an identified or identifiable physical person.

The bill is based on five cumulative control systems: internal control; law; a right of data access and correction by the data subject; supervision by tribunals and appeal courts; and openness of automated data processing. A consultative Council for the Protection of Private Life will have a supervisory role and investigative powers. Certain categories of sensitive data will either not be permitted to be processed or be strictly regulated.

The Main Provisions

The summary below follows the order of the statement of principle of the file cumulative control systems drawn from the official memorandum explaining the bill. But the Chapters in the bill are also indicated to facilitate reference to the bill's text, which is attached to this report as an appendix.

Internal control (Chapter IV)

The data owner will have a duty to:

+ make a record for each name-linked automated data-processing operation -- the nature of the data, the purpose of the operation, the type of links between different data elements, and the persons to whom the data has been transmitted;

+ ensure that the data-processing operation conforms with the declaration made to the Ministry of Justice;

+ ensure that the information on file is kept up to date -- correcting or deleting data that is incorrect, incomplete, irrelevant to the purposes of processing, or obtained or processed without regard for the law;

+ see that access to the data is limited to those who need it for their work and that they cannot make unauthorised modifications.

Data subjects' rights (Chapter II)

When data is being collected, the data subject must be informed at the same time of the following: whether giving the data is compulsory or voluntary; the consequences of refusing to give either part or all of the information; the purpose of collecting the data; and the people or categories of people who will be able to obtain the data. However, these requirements do not apply to industrial and commercial enterprises collecting name-linked data that is not to be communicated to third parties. These rules apply to all name-linked data collected in Belgium, even if the data processing takes place outside the country. It is also forbidden to collect data in Belgium for processing outside the country if such processing would be banned in Belgium because of its sensitive nature.

It is forbidden to process name-linked data that directly or indirectly makes evident an individual's racial or ethnic origin, his sexual habits, political, philosophical or religious opinions or activities, or membership of a labor union or mutual insurance organization. However, such organizations may keep records of their members.

In addition, royal decrees will in exceptional circumstances give details of the types of sensitive data that may be processed and its uses, if the data user receives the written permission of the individuals affected.

Rights of access and correction (Chapter III)

The data subject must be told of his rights of access and correction to records on himself. The data subject must prove his identity, and then the data must be released in an easily understood format, indicating to whom it has been communicated in the previous 12 months. The above information must be supplied to the data subject within 30 days of his making his request. The data owner may charge a fee -- a maximum charge will be set later by royal decree -- but need not handle an individual's request more than once a year. Data subjects will not have these rights regarding the files which doctors, lawyers or bailiffs hold on them.

Tribunals and courts (Chapter III)

The data subject must also be informed about his right of recourse to law if he is dissatisfied with the response of the data owner to his requests. However, he must wait 30 days after his original request, as in the case of access and correction, to give the data owner a chance to reply before taking his case to the tribunal, the first-level court.

The tribunal, in open court, has the power to order the data owner to grant access to a data subject, to correct data and to inform third parties to whom the data has been communicated of the corrections. When a file is corrected in these circumstances, the application fee is reimbursed. When data is subject to judicial dispute, it must be marked as such when being communicated to third parties.

Penalties (Chapter VII)

Penalties include fines of Bfr1,000 to Bfr500,000 (Bfr43=$1) (multiplied by 60 because of indexation) and/or three months to five years in prison, for a person who:

+ communicates name-linked data to a third party knowing that it was not intended to be communicated to that party; and

+ intentionally uses the automated processing of name-linked data in a way not conforming with the intention of that processing operation.

Other penalties include deletion of data, confiscation and destruction of tapes and discs, and banning the use of computers. The court can order the responsible person to be banned from managing either directly or indirectly, for two years or more, a name-linked

data-processing operation. In addition, the court can order the publication of a judgment in full or in part in the press, to be paid for by the guilty data owner.

Openness of automated data processing (Chapter V)

Before a data owner begins the processing, modifying or deletion of automated name-linked data, he must register with the Ministry of Justice. The register will be open to the public, and each processing operation will require a separate registration. Details to be registered will include the following:

+ method of data collection;
+ data-processing system;
+ uses of the data processing;
+ department(s) responsible;
+ links between the data and the conditions under which it would be transferred to third parties;
+ categories of people who have access to the data; and
+ the security system for protecting the data.

If name-linked data is to be exported, or data is processed in Belgium after initial processing in another country, the registration must include additional details:

+ the categories of data to be exported;
+ for each category of data, the country of destination; and
+ if necessary, the intermediate countries through which the data will be transmitted.

Further details required for registration include the following:

+ names and addresses of those registering;
+ name of the data-processing operation;
+ objectives of the operation;
+ purpose of the name-linked data in relation to the objective of the data-processing;
+ categories of people allowed to obtain the data and the conditions under which this will occur;

+ the means by which people will be informed about data on them and how they may exercise their rights of access to it; and

+ the period beyond which the data will no longer be kept, used or transferred elsewhere.

Companies processing data only for internal use will be able to submit a simplified registration form to the Justice Ministry. Although communications between head offices and branches will be considered internal, those between a holding company and a subsidiary will not.

The Council for the Protection of Private Life (Chapter I)

This body will have a general overview of the working of the law, such as review of enforcement procedures, and will make an annual report to the legislature. The council will be consulted by the ordinary civil or criminal tribunals, which will handle legal disputes, and so will develop expertise in this area. However, it probably will not have wide-ranging investigatory powers like the data authorities in Sweden, Norway and France.

Exporting name-linked data (Chapter VI)

The law will apply to transborder data flows in that it will cover automated name-linked data exports as well as nonautomated name-linked data organized with the object of being processed abroad. The law also applies to a data-processing operation abroad which is directly accessible in Belgium via a terminal.

A royal decree will set general conditions for the export of name-linked data and may ban it if the interests of the data subjects would be infringed. In addition, prior approval will be needed for the export of name-linked data for each exporting organization. Penalties for improper data exports range from three months to two years in prison and/or a fine of Bfr100 to Bfr100,000 (multiplied by 60 because of indexation).

When Belgium ratifies the Council of Europe Convention -- which it will do by means of a separate bill after the legislature approves the data-protection bill -- data exports to other ratifying countries will be simpler.

AN OVERVIEW OF PORTUGAL'S DATA PROTECTION BILL

Timetable

Portugal may pass a data protection law in 1987. The government tabled a data protection bill in the Portuguese legislative assembly in early 1984. On May 23, 1984, the parliament approved ratification of the Council of Europe Convention and aimed to pass the law by July. But debate on the bill was delayed. However, the data protection bill is again ready to be debated in the current legislative session.

Scope

The bill covers the public and private sectors, natural persons and automated records. The Justice Minister, Mario Raposo, sees the bill as part of Portugal's strengthening of democratic rights at a time when the police, public administration and major companies are increasingly computerizing their name-linked records.

The bill has been drafted to conform with the Council of Europe Convention, which will be ratified by the time the law is passed. The government expects that the assembly will pass the bill to the Council of Ministers for final approval, which will be followed by the President's ratification.

As this process could take several months, companies and trade associations wishing to influence the debate should contact friendly members of the legislature without delay. When the bill is passed, it is likely that there will be an interval of at least six months before it comes into force. Companies will need this period to prepare themselves for implementing the law.

The main provisions

The data protection law will require all organizations with automated name-linked files to register them and their purpose with a newly established National Commission for Data Protection -- NCDP -- (Comissao Nacional de Proteccao de Dados). Several organizations have been given a voice on the NCDP. The head of the NCDP will be elected by a two-thirds majority in the assembly, and the other six members will be nominated by the President (two), the Ministry of Justice (two), the superior council of magistrates (one) and the public council of attorneys (one).

As the law's provisions may well require companies to change their current record-keeping practices, they should note the following provisions:

Data collection

There will be a ban on the collection or storing of name-linked data on individuals' political or philosophical views, par-

ty, labor union or religious affiliations. But this data may be collected for research or statistics where individuals are not identified, and organizations may keep automated records on their own members.

There will be a ban on the collection or storage of other sensitive data such as an individual's race, sexual habits, criminal records, financial situation, except for public services and with the authorization of the NCDP. Again, this data may be collected and processed on an anonymous basis for research and statistical purposes.

Right of access

Data subjects, people on whom automated data is being collected, will have a right to know whether a file exists on them, the purpose of the file before they are registered on it and the name and address of the data file owner. They will also have the right to gain access to a data file on payment of a fee, a right of correction and a right to have their complaints resolved within 30 days by the organization holding the data. If data subjects have difficulty obtaining these rights, they may take their complaints to the NCDP.

Role of company data protection controller

Companies have a responsibility under this bill to appoint a data protection controller who will take legal responsibility for his company's complying with the law. He will implement company policy on:

+ data collection, purpose, storage time, keeping files up to date,

+ ensuring that they are used only for the purposes registered by the company with the NCDP,

+ informing data subjects of the existence of a file on them, their rights of access and correction.

Role of the NCDP

The NCDP will oversee the law, handle complaints, give advice, prepare a code of conduct for data processing and publish an annual report. Specifically, the NCDP will authorize the registration of automated name-linked data files in the form of a decree for public sector files, and in the official gazette for private sector files. This will mean publication of:

+ the name of the organization's data controller,

+ the way in which the data will be collected,

+ its purpose,

+ its intended storage time,

+ the means by which a data subject may know about and gain access to a file, and

+ how errors may be corrected.

The NCDP will give advice about creating, changing or storing public sector files. In exceptional cases, the NCDP will authorize the linking of separate automated name-lined data files. But public information may be shared among entities with the same purpose, although the term, "public information," is limited to the data on a birth certificate.

Sanctions

In cases where organizations are found to be breaking the law, the NCDP must make the facts public, and may close down data processing operations. Furthermore, the NCDP must report infringements of the law to the Public Attorney Ministry and the courts.

The courts remain an ultimate recourse when problems cannot be resolved by the NCDP. Sanctions under the law for improper use of name-linked automated data files range from 30 days to two years in prison and/or fines.

Name-linked data exports

Transborder data flows are covered by this bill. The Ministry of Justice says it will follow common norms established by the countries ratifying the Council of Europe Convention. Detailed Portuguese procedures have not yet been worked out.

Implementing the data protection law

Once the data protection bill has passed into law, companies should inform the NCDP of new and existing automated name-linked data files within 90 days of the law's official publication. The government has set itself the task of drawing up detailed implementing regulations within six months of the law being passed.