## 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.