Belgium passes four decrees complementing the 1992 Act

In February and March this year Belgium passed four Royal Decrees which details the provisions of the *Act on the Protection of Privacy Regarding the Processing of Personal Data* of 8th December 1992 (PL&B June 1993, p.8). The four Decrees regulate in more detail conditions for processing of sensitive data; conditions for processing of judicial/criminal conviction and related data; data controllers' duty to notify data subjects; and registration fees. The Decrees entered into force on 1st of March this year.

Sensitive data decree

The Act of 1992 provides that processing of sensitive data is only permitted for such purposes as laid down by law or other statutory instrument. The Act leaves it to a special Decree to provide special conditions where processing of sensitive data is allowed.

Sensitive data is defined in Art. 6 of the Belgian Act as personal data regarding race, ethnic origins, sexual behaviour, beliefs, political, philosophical or religious opinions, membership or a trade union or health insurance organisation.

The sensitive data Decree provides for special cases and conditions in which processing of various categories of sensitive data is permitted. There are two groups of these cases:

1. cases of *general authorisation* which apply to processing of all categories of sensitive data;
2. cases of *specific authorisation* which apply only to processing of particular categories of sensitive data.

Generally permitted processing
Processing of sensitive data will be allowed in the following cases:

- it is necessary for complying with a legal obligation;
- it is necessary for complying with an obligation imposed by laws of the countries which are parties to the Council of Europe Convention on Protection of Personal Data 1981, which ensures an equivalent level of protection;
- it is necessary for taking a decision at the request of a data subject;
- it is necessary for providing a service in favour and on request of a data subject;
- it is necessary for satisfying a legitimate interest of a data subject and the purpose of processing is to provide him/her with a real advantage. In this case, the data subject has to be notified of the processing of sensitive data;
- the data subject has consented to processing of sensitive data in writing, after he has been notified of the processing.

Special cases of permitted processing
These are the cases where circumstances make it permissible to process particular categories of sensitive data. Processing of the following categories of sensitive data will be allowed:

- data relating to *racial or ethnic origins*, providing the purpose of processing is identification of data subjects or elimination of discrimination;
- data revealing *sexual life*, providing processing is carried out for medical purposes within appropriate institutions and the data relates to patients and clients of that institutions, or to other persons mentioned by those patients or clients;
- data revealing *political, philosophical or religious opinions or activities, or trade union or insurance organisation membership*, providing data controller is a political party, a philosophical or a religious organisation, trade union or insurance organisation or the data subject is a public figure;
- data necessary for *opinion polls*, providing the data subject has consented and data has been anonymised within six months of collection.

The need for additional guarantees
The Decree explicitly states that sensitive personal data cannot be used in the context of processing for recruitment and job promotion purposes. However, this data can still be processed if, due to the nature of a job or its position, the data represents a fundamental criterion for recruitment or promotion. Also, there are no restrictions, other then those linked to the purpose of data, for processing of sensitive data which has been

communicated spontaneously and in writing by data subjects themselves.

The Decree provides for certain technical and organisational measures which have to be taken by data controllers in the course of their legitimate processing of sensitive data. Thus:

- a data controller has to specifically *appoint* within the organisation employees who are involved in processing of sensitive data and have a *list of these persons,* available for inspection by the data subject and the Commission for Protection of Personal Privacy;
- every employee involved in processing sensitive data has to be subject to a *duty of confidence*, deriving either from a legal obligation, self-regulatory instruments or contracts;
- preliminary *declaration of processing activities* has to include mention of the legal or other statutory basis permitting processing of sensitive data.

Decree on duty to notify data subjects

The Belgian Act in Art. 9 requires a data controller to notify a data subject of the processing of personal data when data is processed for the first time. This notification has to include information about: the identity of the controller, the legal provision authorising the collection of data, the purpose of processing, the possibility to obtain supplementary information from the public register, and the data subject's right of access and rectification. Notification is not necessary where a data subject has been informed of the above at the time of collection, or where processing takes place either within a contractual relationship or any other relationship between the data subject and data controller regulated by law.

The Decree provides for additional exemptions from the duty to notify the data subject of processing and envisages a special procedure of collective notification in certain cases.

Exemptions from the duty to notify

Data subjects do not have to be notified of the processing in the following cases:

- the data subject has *already been notified*, although there was no duty to do so, providing the purpose of the processing has not been changed since;
- the purpose of the processing is *to identify persons who are recipients of public relations activities* of the data controller and to establish or maintain a directory containing explicitly listed categories of their contact information;
- the purpose of the processing is *to identify persons with whom data controller has professional or social relations* due to their activity and to establish or maintain a directory containing explicitly listed categories of contact information of such persons;
- the purpose of processing is to set out *a record of the legal system's jurisprudence* where the judicial decisions are quoted by reference to names of the parties involved, providing the personal data relates to the names of the parties, the purpose of decisions and a summary of them;
- processing is necessary for the *activities of an association or a public body* whose statutory objectives consist in defence and promotion of human rights and fundamental freedoms.

Collective notification

The Decree ingeniously provides that in certain cases, rather than notifying each data subject individually, the data controller may comply with the notification requirement by a collective notification including all or a certain group of data subjects. These are by definition the cases where individual notification would not be reasonable and proportionate in terms of time and cost.

Collective notification is allowed in the following cases:

- where *personal data relating to an individual can be retrieved only by reference to a natural or legal person* and is not done by a search based on data identifying that person and where it is not possible to systematically find data relating to that person;
- where *data is made public by data subject* and is used solely for a purpose related to the original volunteering of data by the data subject;
- where *data processed originates from a judicial decision* which by law has to be publicised, providing the purpose of processing is solely linked to such publicising;
- where data is already processed at the time of entry into force of the Decree and the purpose

of processing is exclusively *business prospecting and list brokering*, providing the data controller does not have direct contact with the data subjects and does not hold any sensitive personal data.

The Decree determines the procedure of collective notification which has to be followed by a data controller in the above cases.

Regarding the first three cases of collective notification, the data controller has to publish information which should have been included in individual notifications, together with the criteria determining the choice of data subjects. This information has to be published in easily understood language in the Belgian official journal and in four journals or periodicals available in the data subjects' domicile. This procedure has to be repeated at least once every five years.

Regarding collective notification in the case of business prospecting and list brokering, the Decree envisages a different procedure. The information which should have been included in the individual notification, as well as the criteria determining the choice of data subjects, has to be broadcast on all the existing general interest channels of Belgian television. This has to be done in easily understood language during three consecutive days at the time of highest viewers' and listeners' coverage.

Decree on "judicial data"

This Decree complements Art. 8 of the Belgian Act which deals with processing of personal data relating to judicial and similar decisions, in civil, administrative and criminal matters. The comprehensive list of these particular categories of data is given in Art. 8 of the Act.

The Decree regulates in more detail the precise conditions under which these categories of data may be legitimately processed by public and private bodies.

Police and other public authorities with a similar function (such as in the area of money laundering) may process judicial and other related data where it is necessary for the pursuit of their policing function. They are also allowed to communicate such data abroad in the framework of international police co-operation. However, the Decree sets a number of conditions for the type of data to be communicated and the circumstances which have to be fulfilled to allow for transfer of these special categories of data abroad.

In addition to police and related public sector processing of data, the Decree explicitly lists the cases where processing of judicial data can take place within other organisations, both in the public and private sectors.

Thus, processing of judicial and other related data is allowed only where it conforms to the following objectives, criteria and conditions:

- processing is carried out for the sole purpose and by an association or a public body whose statutory objectives are defence and promotion of human rights and fundamental freedoms;
- the purpose of processing certain categories of data is to record legal decisions where they

The latest news from Belgium

Organisations in Belgium have started to declare their processing activities to the Commission on the Protection of Personal Privacy. The registration forms have been published together with the Decree regulating the registration fees.

The deadlines for declaring personal data processing operations have now been firmly set and confirmed. Any new processing has to be declared as of 1st of March 1995, the date of entry into force of the four Royal Decrees. Organisations already processing personal data on that day have a deadline until the last day of November 1995 to declare their existing processing activities.

The Commission on the Protection of Personal Privacy is currently preparing two explanatory notes for data users. The notes deal with various issues of interpretation and compliance with particular articles of the Act. The first note is on the relationship between Articles 4 and 9 on the duty to notify data subjects. The second note deals with Art. 18 on keeping of the public register of registered data controllers by the Commission and its links with Art. 10 on data subjects' right of access.

Finally, the Belgian Act refers to a Royal Decree in the area of transborder data flows regulating in greater details conditions for transfers of personal data abroad. The Decree is expected to contain a list of countries which are considered as providing a level of protection equivalent to that of the Belgian Act. This Decree has not yet been passed.

are quoted by reference to names of the parties involved.

In addition to the above cases, processing of judicial data is allowed if it is necessary:

- for execution of a *legal obligation*;
- for execution of an *obligation imposed by a law of a country party to the Council of Europe Convention* on Protection of Personal Data 1981 which ensures an equivalent level of protection;
- to take a *decision at the request of a data subject*;
- to provide a *service in favour and on request of a data subject*;
- for execution of an *obligation imposed by international public law*.

In these particular cases, a data controller has to ensure that the data subject is notified in writing of processing of such data at least one month before the start of processing.

Finally, judicial and other related data can always be legitimately processed where the data subject has consented to it in writing.

Safeguard measures

Where the processing of judicial data and other related data is legitimately carried out in one of the above situations, data controllers still have a duty to take adequate safeguard measures. The Decree mentions the same type of measures as envisaged in the Sensitive Data Decree (see above). In addition, there is a special provision regarding international police co-operation, requiring the data controller to keep a record of all communications of judicial data abroad in the previous six months.

Registration fees

The registration fees range from 1,500 Belgian francs (£33) to 10,000 Belgian francs (£217), depending on the purposes of processing and the form in which the declaration is made. Generally, fees for a declaration presented by automated means are lower than for the cases where declaration is made by filling in the paper forms.

This report was written by Bojana Bellamy, a *Privacy Laws & Business* consultant.

A German DP Commissioner's view on the role of a company data protection officer

Dr. Astrid Breinlinger, Data Protection Commissioner for the land of Hesse, discusses the role of the data protection officer as provided for in Chapter III of the German Data Protection Act (BDSG). This report is based on her article in the German journal *Recht der Datenverarbeitung* [1].

The legal base for the German model

According to Section 36 of the BDSG, private bodies engaged in the automated processing of personal data and regularly employing at least five employees for this purpose need to appoint an internal data protection officer. The main responsibility of the data protection officer is to enforce and audit data protection compliance within the organisation.

The underlying rationale of the German approach is self-regulation, since in the exercise of their duties, data protection officers work in close co-operation with those involved in the processing of personal data and *"with particular reference to the situation prevailing in this area and the special data protection requirements arising therefrom"* [Section 37(1)2].

The Act also makes legal provisions for a relationship between the company data protection officer and the relevant land data protection authority for the private sector. According to Section 37(1), data protection officers may in the exercise of their duties *"apply to the supervisory authority in cases of doubt,"* in order to get an official point of view in controversial matters. On the other hand, the company data protection officer is present when the supervisory authority monitors and checks in specific cases the application of the BDSG and other data protection provisions as stipulated by Section 38(1) and (2).

The duties of the data protection controller - in law and in practice

The duties of the data protection officer as laid down in Section 37 of the BDSG are to ensure the observance of data protection law and other relevant provisions. In three subsections the