Belgian Royal Decree explains Data Protection Law

Report by Sophie Louveaux

BELGIUM'S NEW DATA PROTECTION Royal Decree, adopted on 13th March 2001, introduces important clarifications to the data protection law, adopted in December 1998, which implemented the EU Data Protection Directive. The new law takes effect six months following publication of the Royal Decree.

Although the Royal Decree deals with several areas left open by the previous law, it has not tackled such issues as data transfers to third countries. These issues will be dealt with by a subsequent decree. (A Royal Decree elaborates on certain aspects of a law and is similar to subordinate regulation in other legislative models.)

FURTHER PROCESSING FOR HISTORICAL, STATISTICAL OR SCIENTIFIC USE

To comply with the EU Directive, Chapter II of the Decree establishes various safeguards enabling data controllers to store personal data for longer than required for the initial purpose in order to permit historical, statistical or scientific uses.

The scope of the Decree is limited in the sense that it concerns only further processing for historical, statistical or scientific purposes not considered compatible with the initial purpose. Note that "statistical purposes" covers statistics used not only by the public sector but also by the private sector, such as market surveys.

ANONYMOUS DATA

The main principle established by the Decree is that, whenever possible, only anonymous data may be processed for historical, statistical or scientific purposes – that is, data that cannot be linked to individuals. If it is impossible to achieve the ultimate purpose using anonymous data, then researchers may use encrypted data (that can be linked to individuals) but only by possessing the decryption keys. Similarly, if it is impossible to achieve the purpose with encrypted data, then researchers may use unencrypted data. Of course, the regime becomes progressively stricter as processing moves from anonymous data to unencrypted data.

PROCESSING ENCRYPTED DATA

Data controllers who want to process encrypted rather than anonymous data must justify their reasons in their notifications to the Belgian Data Protection Commission (Commission de la Protection de la Vie Privée or CPVP). Controllers may need encrypted data if, for example, they need to be able to link results to specific individuals.

Data must always be encrypted before it is processed for historical, statistical or scientific purposes. The encryption must be carried out either by controllers themselves (such as a university hospital which encrypts the data before communicating it to researchers) or by a processor or intermediary organisation. The controller may never convert encrypted data into unencrypted data and must establish specific measures to prevent the data being converted.

The law also lays down further requirements for processing special categories of data such as sensitive, judicial or medical information. Should data require further processing for historical, statistical or scientific purposes, the entity encrypting the data must first inform the data subject of the controller's identity, the categories of data processed, and the precise purpose of the processing – unless providing such information proves impossible or requires disproportionate efforts. In the latter case, the organisation's notification to the CPVP must provide such additional information as the precise definition of the purpose, the motives for processing sensitive data and the impossibility of informing the data subject.

PROCESSING UNENCRYPTED DATA

Once the data controller has proved to the CPVP that it could not achieve its purpose with encrypted data, the Decree requires the data controller to obtain informed and express consent from the affected individuals' before processing their data for historical, statistical or scientific purposes. There are two exemptions. The first occurs when the unencrypted data is publicly available (that is, the data subject has made it publicly available or the data is directly related to the public nature of the person or the facts in which he/she has been involved). The second exemption allows processing if it is impossible to obtain the data subject's consent, or obtaining consent

requires disproportionate efforts. In the latter case, the data controller must obtain an exemption from the CPVP according to the specific procedure set out in the Decree.

Publishing results

The Decree forbids publishing the results of historical, statistical or scientific data processing in a form that enables others to identify the individuals unless they have consented to the publication and the results do not affect the privacy of a third party, or the data is publicly available.

Processing special categories of data

The Decree establishes safeguards for processing sensitive, judicial or medical data. These include obliging a data controller to prepare a list, accessible to the CPVP, of those having access to the data and their precise function concerning the data (such as nurses on a ward having access to medical data about patients in their care). Data controllers must not only inform data subjects that their data will be processed. They must also indicate on which legal grounds they base the processing. If the controller will rely on data subjects' consent to process sensitive or health-related data, then the controller must also tell the individuals who will have access to the data.

Finally, the Decree provides that individual consent does not lift the prohibition against processing sensitive or health-related data if the data controller is the data subject's current or potential employer, or if the data subject is dependent on the controller in some way. However, the prohibition may be lifted if the data processing is intended to grant the data subject an advantage (for example, an employer collecting data on employees' religious beliefs to set up a chapel on company grounds).

Exemptions to the right to be informed

To conform with article 11.2 of the Directive, the Decree establishes some conditions that exempt the data controller from the general obligation to inform the data subject. These conditions include when the data has not been collected directly from the individual and is being used for statistical, historical or scientific purposes, or when informing the individual proves impossible or involves disproportionate efforts.

If the data is processed further for statistical, historical or scientific purposes, the controller need not inform the data subjects providing he/she respects the regime spelled out in the Decree. In other cases, when informing the subjects proves impossible or requires disproportionate efforts, the controller need not inform the data subject unless the controller establishes contact with the individual, or the individual communicates with the data controller. Similarly, any third parties receiving the data must inform the data subject when and if they establish contact with the individual. In its notification to the Commission, the data controller must substantiate its contention that informing individuals proved impossible or required disproportionate efforts.

Exercise of right of access, correction and opposition

The Decree sets out the means for individuals to exercise their rights of access, correction and objection.

Individuals may exercise the right of access and correction simply by sending a dated and signed request with proof of identity to the data controller or representative in Belgium, either by post, by hand, or by any form of telecommunication (such as telephone or e-mail).

Individuals may exercise their rights to object to the processing of their data in different ways depending on how the data is collected. If the data is collected directly from the individual in writing, that document must contain a clause enabling the individual to oppose the processing. If the data is collected orally, the data controller must ask the individual whether he/she wishes to object to the processing, either in a written document sent to the person within two months of the collection, or using any other technical means by which it is possible to establish that the data subject was given the opportunity. When the controller collects the information indirectly, the controller must advise the individuals in writing, enabling them to object to the processing.

Indirect access

The Decree lays down the procedure individuals must follow to gain access to information held by entities such as the police, state security and National Defence. In these cases, individuals must exercise their right of access through the CPVP, which serves as an intermediary between them and the relevant entity. Thus the individual will not gain direct access to the data. The CPVP will only inform the data subject that the processing complied with the law, without providing any further information about either the quality of the data or the purposes for which it is processed.

Notification and Public Register

The Decree establishes the fees the data controller must pay when notifying the CPVP of the processing and gives clear preference to notification in electronic format.

The Decree also establishes exemptions to the obligation to notify, including (under certain conditions) a company processing data for its own staff administration or accounts, administration of data concerning its stakeholders, or its clients/retailers for accounts and records.

Finally, the Decree establishes the means for individuals to access the Public Register of data processing notifications held by the CPVP.

Sophie Louveaux may be contacted at e-Consult, 21 avenue Baron Fallon, 5000 Namur, Belgium
Tel: +32 (0)81 40 36 36
Fax: +32 (0)81 40 36 35
http://www.e-consult.be