Luxembourg finally adopts data protection law

By Lilly Taranto

IN SEPTEMBER 1999, the European Commission started proceedings against Luxembourg for non-transposition of the EU Data Protection Directive. Three years later, and after a four-year delay, Luxembourg adopted its new data protection law on August 2nd 2002.

HISTORICAL BACKGROUND

Long before the new law, Luxembourg was one of the first European states to have implemented data protection legislation. The data protection law of 1979 ensured better protection of personal data against cases of abuse, and provided that preliminary authorisation (a kind of formal written consent) from individuals was required before organisations could process their details.

However, due to the advent of the information age and the increasing ability to process, manipulate and transmit personal data, the 1979 law became obsolete.

THE NEW LAW OF AUGUST 2ND 2002

In today's global information society, cross-border data flows allow for freedom of expression, information and trade. Yet there are fundamental human rights implications attached to these data flows. Luxembourg's new law ("Protection des Personnes à L'égard du Traitement des Données à Caractère Personnel") along with the EU Data Protection Directive, sets a balance between the information society's dependence on free movement of personal data, and the protection of the fundamental rights of individuals.

Awareness of the information society's reliance on the processing of personal data made it necessary to replace the 1979 law's consent provision with a uniform procedure of notification. Under the new data protection law, data controllers are now required to notify any processing of personal data with the National Commission for the Protection of Personal Data, which is then able to verify legal compliance. However, the law still required the old system of preliminary authorisation to be sent to the Commission in situations where the processing may cause an intrinsic risk to the data subject's privacy. Because this is a new law, however, there are no precise definitions as to what exactly is meant by "intrinsic risk".

The main objective of the law is to set a common rule for private and public organisations when processing personal data that takes into account the technological developments that have occured since the previous 1979 law was passed. This new rule specifies that:

- any data processing has a purpose
- the data subject is informed
- data is used only for the initial purpose of the processing; and
- data is destroyed once the purpose of the initial processing has been achieved.

The scope of the new data protection law is wider than the EU directive. Its provisions apply also to:

- legal persons, public organisations, and the realms of defence, public and state security, and criminal law proceedings
- genetic data – created as a new category within sensitive data
- data processing for the purpose of surveillance and, in particular, for the purpose of surveillance in the workplace; and
- the sharing of personal data between organisations.

The law does not apply to personal data collected during the course of an individual's private activities.

DEFINITION OF PERSONAL DATA AND DATA SUBJECTS' RIGHTS

Article 2 of the law defines personal data as information regarding an identified or identifiable person. The most important aspect is that data is *personal*, regardless of its form or how it is stored. This renders the provision technology-neutral and, therefore, applies to both manual and computerised data.

Article 5 provides that data processing, whether automated or manual, is legal if:

- it is kept confidential and secure
- it is adequate and relevant in relation to the purpose of processing
- the processing has a purpose
- the data subject is informed

• data is used only for the purpose of the initial processing; and

• data is destroyed once the purpose of the initial processing has been achieved.

The law also explains the data subject's rights. These include the right to be notified of any processing, access to personal data, and objection to further processing. Concerning the right of notification, the law requires the data controller or processor to be identified. The controller or processor must inform the data subject that their details are being processed. Exemptions to this right include public and state security, or the physical safety of the data subject or a third party.

An individual's right of access to personal data includes the right to be informed that their details are being processed. It also includes the right of rectifying inaccurate or false data. Exemptions to this right are the same as those for the notification right.

Finally, regarding the right of objection, the law allows individuals to exert this right unconditionally when data processing occurs for commercial or political purposes.

Sensitive data

Like the EU directive, Luxembourg's law prohibits the processing of sensitive data, except for certain exemptions. Moreover, the law extends this prohibition to include genetic data; a form of sensitive personal data that is being increasingly collected and manipulated by organisations.

Sensitive data may be processed only in the case of an individual's express consent. However, the law sets out certain exemptions to this rule, for example:

• obligations set out by labour law

• medical emergency

• justice and defence

• relevant public interests, such as those connected to historical, scientific and statistical issues; and

• public and state safety.

Genetic data rules are even stricter, with processing allowed only in listed circumstances such as:

• when the processing is necessary for the safety of the data subject or third party, or when the data subject is incapable of giving consent

• when the processing is necessary for the exercise and defence of justice

• in case of relevant public interests such as historical, scientific and statistical issues; and

• in the cases indicated by Article 17 – defence, public safety and criminal law proceedings.

Finally the law sets out special provisions for the processing of health and judicial records.

Freedom of expression

According to the law, freedom of expression is a wide concept including artistic and literary expression, which includes journalistic expression. Using their discretion, journalists are not obliged by the law to inform the data subject of the processing. Right of access is also limited. Moreover, the National Commission for the Protection of Personal Data may investigate only in the presence of the press representative body.

Processing of surveillance data

The processing of surveillance data for law enforcement purposes, or for monitoring in the workplace, is permitted only in the following cases:

• with an individual's express consent

• the state's intervention for reasons of public safety; and

• when surveillance occurs on private premises.

It is compulsory to inform the public when surveillance is taking place. In addition, provided that an individual has given express consent, data can be transmitted to public and judicial authorities.

As far as surveillance in the workplace is concerned, the law allows the compulsory use of surveillance in the following situations:

• employees' health and security

• company protection and welfare

• control of mechanical/computerised production; and

• monitoring employees' work activities in order to calculate their wages.

These provisions do not require the employee's consent, but the law does require organisations to inform employee representatives and the minister of labour when surveillance is being used and for which purposes.

Telecommunications exemptions

Article 41 of the Law provides exemptions for postal and telecoms operators when passing on customer details to third parties with a legitimate interest (eg. law enforcement agencies). Legal authorities, such as judges, are given the power to verify the legitimacy of such requests. Telecoms operators are able to avoid any legal liability through the use of 'black box' technology. This technology allows an organisation (with the correct permission) to immediately access a particular customer's data without the telecoms provider being able to identify either party.

The National Commission for the protection of personal data

The law establishes the National Commission for the Protection of Personal Data, an organisation which is independent from the government. The Commission's internal regulation was passed on November 29th 2002. Article 32 of the Law describes the duties and powers of the Commission. These include:

continued on page 16