Data laws change fast in Hungary, Estonia and Slovenia

Nowhere is the legal environment for processing personal information changing more quickly than in the former communist states of Eastern and Central Europe. In the wake of the fall of the Soviet empire, no fewer than ten countries (either former Warsaw Pact members or ex-Soviet republics) have turned their attentions towards the West by submitting applications to join the European Union. Nick Platten reports on the fast-changing situation in three of the more advanced countries (in data protection terms) Hungary, Estonia and Slovenia.

For five of these 10 countries (Poland, Hungary, Estonia, Slovenia and the Czech Republic), the European Commission has recommended that negotiations on accession to the EU be opened. The remaining five (Lithuania, Latvia, Slovakia, Bulgaria and Romania), if the Commission opinion is followed, will need to wait a little while longer, but nevertheless will be part of a "reinforced pre-accession strategy."

Of course, membership of the EU requires the adoption of the whole raft of Community legislation. With the adoption of the general Data Protection Directive in 1995, an important part of this "acquis communautaire" now relates to privacy and data protection. In recent years, the candidate countries, many of which had no existing laws in this area, have therefore been busy developing law.

Hungary

Hungary has perhaps the most developed data protection regime of all the Central and Eastern European countries. Data protection features in the Hungarian constitution, there is a well-established law (PL&B Sep '95 p.3), and, virtually alone among these countries, a developed and operational supervisory authority in the form of the independent Data Protection Ombudsman (PL&B May '97 p.18). The Hungarian Constitution includes in Article 59 (in the chapter on the Basic Rights, Freedoms and Duties) a guarantee that "everyone has the right to the good standing of his reputation, the privacy of his home and the protection of secrecy in private affairs and personal data."

This constitutional provision led to the adoption, in 1992, of Act LXIII - a framework law on the *Protection of Personal Data and the Disclosure of Data of Public Interest*. As can be judged from its title, this law encompasses both data protection and public access to official information - rare in Europe but not uncommon in other parts of the world (Canada, for example).

Since then, a number of sectoral laws have included provisions on data protection, notably in the areas of the secret services, statistics, marketing, scientific research, and, most recently, (May 1997) health data. The adoption of this most recent law enabled Hungary, in October 1997, to ratify Council of Europe Convention 108.

The Hungarian law is comprehensive. It includes the essential features of Council of Europe Convention 108 and, more importantly for Hungary's aspirations to EU membership, much of what the EU Directive requires. It applies to all processing of personal data, including manual files. All the basic data protection principles are present, as well as provisions on sensitive data, transfers abroad, and on the establishment of an independent Ombudsman with appropriate powers.

It would be wrong, however, to suggest that the Hungarian situation is perfect. There do seem to be some weaknesses in the legislation. Most notable is the absence of any significant sanctions for non-compliance with the law's provisions, other than a responsibility to pay compensation in certain circumstances to data subjects.

Enforcement of the law is also weakened by the absence of a real power for the Ombudsman to initiate legal proceedings where a breach of the law is revealed by an investigation. A system of registration is established by the law, but the exemptions are extremely sweeping, and there seems to be no power for the Ombudsman to check the lawfulness of a proposed data processing operation before it begins - a necessity under the Directive for processing wih "specific risks."

As far as individual rights are concerned, the classic rights of access and rectification are present, but the new "add-on" rights provided by the Directive (the right to object and the right not to be subject to an automated individual decision) are absent. The provisions on sensitive data also seem quite generous to data controllers in comparison with those in the Directive, but, on

the other hand, the regime for non-sensitive data seems much stricter, requiring data processing to be legitimised either by law or the consent of the individual data subject.

The law also includes no notion of sub-contracted "processors" or "computer bureaux" which seems to leave a gap in its provisions on security. Also, like many pre-Directive laws, collection of personal data is not considered as "processing." The effect of this is that there is no obligation on data controllers to fix the purpose of the processing at the time of collection.

These negative points are significant, but should not detract from the overall picture of Hungary as a country with a functioning and seemingly successful data protection regime. Changes to the law will probably be needed in the future if Hungary is to accede to the EU, but a data protection legal culture seems to be rooted.

Estonia

In contrast to Hungary, the Baltic state of Estonia is a relative newcomer to data protection. The *Estonian Personal Data Protection Act* was adopted on 12 June 1996 and entered into force on 19 July 1996. It required the establishment of a Data Protection Supervisory Authority by 1 January 1997, and data processing to be brought into line with the Act's provisions one year later.

A data protection department has been established in the Ministry of the Interior, although there is no Commissioner as such. Although the Act was supposed to apply to processing from 1 January 1998, as the department had not received any registrations by then, there are now further transitional periods.

As the law is still not yet fully operational, any analysis of the Estonian situation must be limited to an examination of the text of the law. The Estonian law is, like Hungary's, a comprehensive framework law covering automatic processing as well as manually processed data. The basic definitions such as "personal data," "chief processor" (i.e. data controller) - are modelled quite closely on the Directive, but those expecting a copy of the Directive will also find plenty of surprises and novelties.

"Sensitive data" is split into two different categories, to which different rules apply. For one of these categories (political opinions or religious or other beliefs), Estonian citizens and residents are better protected than foreigners, which seems discriminatory. For non-sensitive data there are detailed rules on disclosures, but not for processing generally. Several of the basic data protection principles (fair and lawful processing, the compatible purpose principle, limits on data retention) are also absent.

On the other hand, the basic individual rights of access and rectification are included, although the data subject only receives information about processing if his consent is needed, and not routinely whenever data is collected. The "add-on" rights provided by the Directive (right of opposition, right not to be subject to an automated individual decision) are, like in Hungary, not included in the law.

Supervision of the law is entrusted to an independent supervisory authority with many of the powers that such authorities in other countries enjoy. However, once again, there is no power to engage in legal proceedings. Where the law is being breached, the authority may issue an order (or "precept"), but it is not clear how compliance with this order will be secured. There are also no provisions on the data controller's (chief processor's) liability to pay compensation.

As far as notification (registration) is concerned, there is a simple split: processing involving sensitive data must be notified, all other processing need not be.

The overall impression is of a law that still needs to be honed a little. It is noticeable that some of the language and concepts of the EU Directive have been taken over, but then not used in the way intended. For example, Article 7 of the Directive (which sets out six alternative legal grounds for processing of all data) seems to have been used as the model for Article 8 of the Estonian law dealing specifically with sensitive data. Nevertheless, for a country with no history of law in this area, the 1996 Data Protection Act is a big step forward and a basis for development.

Slovenia

Of the three countries considered in this report, Slovenia has the longest-standing legislation, with a law dating back to 1990. In addition, Article 38 of the Slovenian Constitution (1991) guarantees "the protection of personal data relating to an individual." The Article forbids the use of

personal data if this conflicts with the original purpose for which the data was collected. It sets out a requirement for the collection, processing and end-use of personal data, as well as the supervision and protection of the confidentiality of such data, to be regulated by statute. It also sets out the right of each person to be informed about the personal data relating to him or her which has been collected, and the right to a legal remedy in the event of misuse of the data.

This relatively detailed constitutional provision supplements and reinforces the Data Protection Act of 7 March 1990, which is the principal piece of existing legislation in this field, and the basis on which Slovenia has been able to ratify the Council of Europe Convention 108.

In recent years, considerable preparatory work has apparently been undertaken to prepare a new general data protection law. However, this new draft law has still not yet been adopted.

Surprisingly, given the relative maturity of the law, little information is available regarding the operational character of the data protection supervisory regime in place in Slovenia, either in the form of case law or reports from the state authority responsible for supervision. This overview therefore focuses exclusively on the Data Protection Act of 1990, and the constitutional provisions.

The first point to note is that the Slovenian law is built around the concept of the *data file,* a term which encompasses both files which are automatically processed and those processed by manual means. This approach now seems dated. Most of the more recent European laws talk of "data processing" rather than "data files", a change intended to reflect the more amorphous nature of modern data and information use.

The law also divides those persons entitled to process information into *data controllers,* a familiar notion, and authorised *users*, a less familiar one. Users do not have all the responsibilities of data controllers, they are not required to register, for example but they are a quite different animal from the *processor* in the Directive or the *computer bureau* of the 1984 UK law. Users are able to process personal data for their own purposes, and are authorised to do so by law or with the consent of the data subject. The basic building blocks of the Slovenian law are, therefore, different to those found elsewhere.

The substantive provisions of the law are also something of a mixed bag. On the one hand, there seem to be some important elements missing. For example, not all of the basic principles (fair and lawful processing, proportionality, accuracy) from Article 5 of Convention 108 and Article 6 of the Directive are present. There are also no specific provisions on sensitive data and no requirements to provide information when collecting personal data. The add-on rights from the Directive (right to object, rights regarding automated individual decisions) are also absent.

On the other hand, the law does include some quite strict provisions which are not to be found in the Convention or the Directive. For example, Article 7 establishes the principle, also found in certain of the Council of Europe sectoral recommendations, that personal data may be collected only directly from the data subject. There are some exemptions, however.

Perhaps the most important issue regarding the Slovenian data protection regime concerns the supervision and compliance system. The law entrusts the role of "supervisory authority" to the state agency competent for the social system's information. It is not clear whether this agency is able to act in the independent fashion which is a characteristic of data protection authorities in most countries, and a requirement of the Directive.

The system of notification (registration) also seems a little old-fashioned, in that there is a universal requirement to register. The system would probably benefit if it were made more sophisticated and tailored to the risks presented by the processing. Provision for prior checking of particularly risky processing could be introduced, while, at the same time, exemptions from notification for non-risky processing could be added.

The Slovenian law and constitutional provisions are a first step in the development of data protection in that country, but the law is already seven years old, and, as the Slovenian authorities seem to have acknowledged in their decision to prepare a new law, in need of some revision.

Subsequent newsletters will cover the situation in other Central and Eastern European countries. Nick Platten is an independent international data protection consultant.