ITALY LIKELY TO ADOPT DATA PROTECTION LAW IN 1994

Italy looks set to enact a data protection law in 1994. After a decade of drafts and proposals (PL&B Oct. 1992 pp. 25/6), the Italian Government finally submitted a new Data Protection Bill to the Parliament on September 1st 1992. Following publication of the revised text of the EC Draft Directive and in order to reflect these changes, in March 1993, the government updated the bill and introduced some amendments. As at December 1993, the amended Bill is being discussed in the Chamber of Deputies' Legal Committee.

The Legal Committee of the Chamber of Deputies has approved the basis of the text as a whole and that the detailed discussion article-by-article would normally follow both in the Legal Committee and in the Chamber of Deputies. However, the Legal Committee has proposed that the Bill should be adopted by the so-called "urgency procedure," which means that detailed discussion should take place only in the Legal Committee and not also in the Chamber. As a result of using this "urgency procedure," it is expected that the Bill will be adopted in 1994.

Here we examine how Italy's Data Protection Bill deals with the key issues.

1. Scope of the Act (Arts. 1 & 2)

Automated and manual data: Italy's Bill covers processing both by automated and manual means. Manual records are covered by the bill as long as they are organised and structured in such a way as to facilitate access to information.

Natural and legal persons: Unlike most of the other European data protection laws, the Bill also covers data on legal persons, for example, companies and organisations. This means that if a company or public administration holds data on other legal entities, the former will have to comply with the provisions of the Italian Bill in the same way as when holding data on individuals.

Public and private sectors: Italy's Bill applies to data processing operations within organisations in both private and public sectors. With minor exceptions, a uniform legal regime is envisaged for both sectors.

2. Data quality principles (Art. 4)

These are the basic principles contained in the Council of Europe Convention 108 and all European national data protection laws. Personal data has to be:

- processed lawfully and fairly,
- collected and stored for specific and legitimate purposes and used in a way compatible with those purposes,
- accurate and up-to-date,
- adequate, relevant and not excessive in relation to the purposes for which it is collected, and
- kept in a form which permits identification of the data subject for no longer than necessary for the initial purposes.

3. Conditions for processing of personal data (Arts. 3 & 10)

Similar to the EC Draft Directive, Italy's Bill includes consent of a data subject as one of the conditions for lawful processing. This means that if a data user can satisfy one of the remaining conditions on the list there is no need to obtain a data subject's consent.

Thus, processing is legitimate if one of the following conditions is fulfilled:

- the data subject has consented to it, or
- it is necessary for execution of a contract with a data subject, or
- it is based on an obligation imposed by national or EC law, or
- data is collected from public sources, or
- data is processed for study, research or statistical purposes, or
- it takes place within the journalistic profession for purposes of journalism.

4. Informing the data subject (Art. 10)

At the time of collection of personal data from the data subject, the controller has to inform the latter of the following information:

- the identity of the controller,
- the purpose of the data processing operations,
- the mandatory or voluntary nature of the data subject's responses,
- the consequences of a failure to reply,
- a third party to whom data may be communicated,
- data subjects' rights of access to and rectification of personal data on them.

5. Sensitive data (Art. 5)

Italy's Bill has adopted the standard definition of sensitive data. Thus, sensitive data is any personal data which may reveal:

- racial or ethnic origin,
- religious or philosophical belief,
- political opinion,
- membership of and activity in any political, trade union, religious, or philosophical organization,
- health or sexual life.

As a general rule, this sensitive data can be processed only with the **express and written consent** of the data subject concerned. However, some exceptions to this rule are envisaged for health care institutions, journalists, and identified public bodies.

6. Registration (Art. 8)

Prior to the commencement of data processing activities, the data controller has to notify the Data Protection Commission (DPC) of any intended processing. This notification has to contain the following information:

- the identity of the data controller or processor (a person who processes data on the controller's behalf), if any
- the purpose of the processing
- the nature of the personal data, places where it is kept and categories of data subjects to whom data will be communicated
- any data security measures
- any connection with or transfers to other countries
- the duration of the period for which data will be stored or communicated.

Any change in the above information would necessitate a new notification to the DPC.

The data user may only commence processing operations 45 days after the date on which the notification was made. During that period, the DPC has the power to verify the notified information and require the adoption of additional measures and adaptations or corrections in the interest of data subjects. The controller has to comply with the Commissioner's requirements.

7. Data subject's rights (Arts. 11 & 12)

Italy's Bill gives data subjects the standard rights of access and rectification and following the example of the EC Directive, adds certain other rights. Thus, data subjects have the following rights:

Right of access to their personal information held by a data controller. Thus, data subjects are entitled to know of the existence, origins and the content of their personal data file and have a right to an intelligible copy of this data.

Right of rectification and deletion allows data subjects to demand blocking and deletion of data processed in breach of the Italian Bill, as well as the correction of inaccurate data.

Right of erasure. Data subjects may demand to have their data erased if it is intended for the purposes of direct marketing.

Right to object to processing. Data subjects may object on legitimate grounds to the processing of personal data on them.

The limited exceptions to these data subjects' rights mainly concern data users in the public sector.

8. Transfers of data to third parties (Arts. 13 & 14)

Transfers of personal data to third parties are permitted under the following conditions:

- if the data subject has consented, or
- if the data comes from public sources, or
- if the transfer is necessary in order to comply with national or EC law, or
- if the data is transferred within the journalistic profession and for journalistic purposes.

The *exceptions* to the above rules are envisaged only if communication and transfer of data is necessary for:

1. research and statistical purposes and the data is held in anonymous form, and
2. for reasons concerning state defence, the prevention and assessment of unlawful acts, or prescribing of sanctions.

In any case, data may be transferred only for the purposes specified in the notification to the Data Protection Commission.

There are special rules for communication and transfers of data within and by the public administrations, and health care institutions.

9. Data security (Art 7)

Italy's Bill imposes an obligation on data users to keep personal data in such a way as to limit to the very minimum the risk of its destruction, loss (even accidental) and unauthorised access. Therefore, the data user has to adopt preventive security measures taking into account the state of technology and the nature of the data.

The minimum security standards are going to be specified in a separate Decree.

10. Transborder data flows (Art. 18)

In order to transfer personal data abroad, the controller has to make **prior notification** to the Data Protection Commission. The actual transfer may take place only 30 days after the date of notification. The Commission may prohibit transfers of data to a country which does not provide an *equivalent level of protection*. In assessing equivalence, the nature of the personal data and the purpose of the processing will be taken into account.

It would be reasonable to expect that most of the European countries with data protection laws would be regarded as providing an equivalent level of protection. However, while this is so regarding the level of protection afforded to *individuals*, the same does not apply to the level of protection of data on *legal persons*, since most of the other European data protection laws do *not* cover legal persons.

11. Sanctions (Arts. 23 - 28)

Criminal sanctions: The sanction of *imprisonment* is prescribed for the following offences:

- failure to notify, or false or incomplete notification
- failure to inform a data subject
- breach of conditions for lawful processing
- not complying with the provisions on sensitive data
- disclosure to third parties in breach of the Bill
- failure to adopt security measures
- not complying with the Data Protection Commission's enforcement notice.

Administrative sanctions: The sanctions of *fines* will be imposed for failure to give requested information to the DPC.

12. Data Protection Commission (DPC) (Arts. 19 - 21)

The DPC is an independent supervisory authority whose President and four other members are appointed from eminent judges and law professors. In addition to the usual monitoring, controlling and supervisory functions, the DPC may, on the basis of complaints received, serve an enforcement notice on data users.

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