Italian data security deadline approaches

Businesses operating in Italy now have a little over three months to comply with new security regulations. **Lilly Taranto** explains what steps they will need to take.

When Italy's Data Protection Code came into force at the beginning of this year, it established a legal requirement for organisations to document their data security practices. Italian organisations were initially given until March 2004 to establish what is known as the 'Programmatic Data Security Document' (PDS), although due to the complexity involved, the Italian Data Protection Authority (the Garante) recently extended the deadline to December 31st.

So what exactly is a PDS, who is required to adopt it, and what does the process involve?

What is the PDS?

The PDS is the only document whose adoption certifies legal compliance with the Italian Data Protection Code. It is basically an internal corporate manual for assessing and planning data security. The adoption of the PDS ensures that companies have assessed internal and external data security measures, identified the main areas of risks, and put in place adequate minimum security measures to avoid damage to, and/or, loss of data. Least but not last, the adoption of the PDS can help to avoid prosecution and regulatory sanctions.

In other words, the aim of the PDS is to assess risk, establish security measures and distribute tasks among personnel to ensure adequate levels of protection for personal data (see box, above). The adoption of the PDS should be based on a detailed audit of the company, its systems and overall functions. A typical PDS will contain around 150 pages and can take from three weeks to two months to draft, depending on the size of the company.

The PDS must be updated every year on March 31st and a copy kept in the company's head office. Although organisations are not required to obtain the Garante's approval, they must have a copy available for inspection by the regulator.

Security document requirements

1. Details on the types of processing

2. Name and job functions of personnel responsible for the security measures

3. Analysis of the security risks

3. List of adopted security measures, which may include among others:

- Password controls for accessing data, which must be made of a minimum of 8 characters and changed every three months
- Encryption
- Firewalls
- Anti-virus software
- Periodical backups
- Description of data protection training for staff carrying out data processing

Who is covered?

All private and public sector organisations processing electronically sensitive data in Italy must adopt the PDS, irrespective of whether their servers are linked up to public networks. This means that virtually all companies must adopt the PDS, as processing of ordinary personal data rarely excludes the processing of sensitive data.

Drafting the PDS requires a detailed assessment of the organisation and its service providers (for example, marketing agencies or call centre providers), data processing systems, methods and the risks involved. Once the assessment has been carried out and the security measures have been put in place, staff must be given security training based on the PDS. Each member of staff should receive customised training depending on the department and the role within the company. The PDS is therefore not just a bureaucratic exercise. It is a real data security plan establishing effective data protection across an organisation's systems and staff.

Incentives to comply

The Garante and the Italian Tax Police (Guardia di Finanza) have recently reached an agreement to intensify controls and apply sanctions where organisations breach the law. Sanctions can include fines up to €60,000 and imprisonment of up to three years.

The agreement represents a strong incentive for companies to adopt the PDS. In addition to the fear of sanctions, it should be noted that most reputable companies operating in Italy have decided to adopt the PDS to obtain certified legal compliance with the law, reduce business risk and ensure competitive advantage over those who have not adopted it.

AUTHOR:

Lilly Taranto, consultant, Marketing Improvement.

CONTACT:

lilly.taranto@marketingimprovement.com

FURTHER READING:

Details on the security regulations can be found in the Italian Personal Data Protection Code:
www.privacy.it/privacycode-en.html

For for previous coverage on the Italian Data Protection Code, see *PL&B International*, October/November 2003, p.24.