PORTOLANO CAVALLO
studio legale

Legislative Decree 69/2012 implements in Italy the e-Privacy Directive 2009/136/EC

May 28, 2012

Laura Liguori and Federica De Santis

On May 28, 2012 the Italian Government issued Legislative Decree no. 69/2012 ("Decree") implementing in Italy Directive no. 2009/136/EC (which amended Directive 2002/58/EC – "e-Privacy Directive").

The Decree, which entered into force on June 1, 2012, amended the Italian Data Protection Code (Legislative Decree of June 30, 2003, no. 196) introducing new requirements for providers of publicly available electronic communications services to deal with personal data breaches and new provisions on the use of cookies by website operators.

Please find below a brief summary of the main measures taken by the Italian government.

* * *

Definition of personal data breach

The Decree amends Section 4 of the Italian Data Protection Code introducing the definition of "personal data breach", meant, in accordance with Section 2(2)(c) of the e-Privacy Directive, as a breach of security leading to the accidental destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed in connection with the provision of a publicly available electronic communications service (new Section 4(3)(g-bis) of the Italian Data protection Code).

Procedures to deal with a personal data breach

The Decree implements in Italy the data breach notification requirements as set forth under the e-Privacy Directive (new Section 32-bis of the Italian Data Protection Code). According to the new provisions:

- in case of a personal data breach providers of publicly available electronic communications services shall notify the personal data breach to the Italian Data Protection Authority ("DPA"), without undue delay;

- when the personal data breach is likely to adversely affect the personal data or privacy of a contractor or another individual, the provider shall also notify said subjects of the breach without delay. However, the notification is not required if the provider is able to give evidence to the DPA that it has implemented appropriate security measures – aimed at making data unintelligible to unauthorized third parties -, and that those measures were applied to the data concerned by the security breach;

- if the provider has not already notified the contractor or other individual of the personal data breach, the DPA may require it to do so, having considered the likely adverse effects of the breach;

- the notification to the contractor or individual shall at least describe the nature of the personal data breach and the contact points where more information can be obtained, and shall list the measures to mitigate the possible adverse effects of the personal data breach. The notification to the DPA shall, in addition, describe the consequences of the data breach, and the measures proposed or taken by the provider to address the same;

- providers shall keep an inventory of the personal data breaches including the facts surrounding the breach, its effects and the measures taken to face the breach. Such inventory will help the DPA to check compliance with the new provisions.

If the provision of an electronic communications service has been outsourced to third parties, the latter shall cooperate with the provider for purposes of compliance with the above notification requirements.

The DPA may issue guidelines and instructions concerning the circumstances under which providers are required to notify personal data breaches, the format of such notification and the modalities in which the notification is to be made.

Failure or delay to notify a personal data breach to the DPA is sanctioned with a fine ranging between EUR25,000 to EUR150,000.

Failure or delay to notify a personal data breach to the contractor or other individual is sanctioned with a fine ranging between EUR150 and EUR1,000.

Providers' failure to keep an inventory of the personal data breaches is sanctioned with a fine ranging between EUR20,000 to EUR120,000.

The above-mentioned notification requirements currently apply only to "providers of publicly available electronic communications services", in accordance with the e-privacy Directive.

However the same e-privacy Directive, in consideration of the fact that interest of users in being notified is not limited to the electronic communications sector, provided that mandatory notification requirements applicable to all sectors and type of data should be introduced at EU level as a matter of priority (recital 59).

The opportunity to apply the data breach notifications requirements to all data controllers has been stressed also by the Article 29 Data Protection Working Party (Opinion no. 1/2011 of April 5, 2011) and by the EU Commission in a public consultation on circumstances, procedures and formats for personal data breach notifications launched on July 14, 2011.

In this regard, the proposal for an EU data protection regulation issued by the EU Commission on January 25, 2012 provides for data breach requirements in relation to any data controllers.

"Opt-in" principle to use cookies

The Decree amends Section 122 of the Italian Data Protection Code clearly providing for an "opt-in" principle to use cookies, i.e. small files that store information on users' hard drive or browser.

In particular, as a result of the implementation of the e-Privacy Directive:

- storing information on users' pc and retrieving said information in the form of cookies is lawful only after having obtained users' consent;

- consent must be informed, i.e. data subjects shall be provided with an information notice which can be simplified according to a resolution to be issued by the DPA;

- consent can be expressed through the settings of a software or other devices.

This shall not prevent any technical storage or access for the sole purpose of carrying out the transmission of a communication over an electronic communications network, or as strictly necessary in order for the provider of an information society service explicitly requested by the subscriber or user to provide the service at issue.

The DPA has not clarified yet how providers can technically obtain users' prior consent to use cookies. It is expected that it will do so in the next few months.