

Assembling the privacy jigsaw: analysing recent amendments

Italy's data protection framework, as set forth by Legislative Decree of 30 June 2003, No. 196 (Data Protection Code), has been significantly amended over the last year. However, the piecemeal approach of the legislature has created uncertainties, noted by the Garante in November 2012, which stated the current system is "complex and difficult to read", requesting that the Italian Parliament and Government evaluate their approach to data protection. Laura Liguori and Federica de Santis, Partner and Associate at Portolano Cavallo Studio Legale, outline the successive changes that have occurred in Italy and what we can expect to see this year.

New definition of personal data and data subject

In December 2011, the Italian Government passed Decree No. 201/2011, converted by Law No. 214 of 22 December 2011, which excluded legal entities from the definition of 'data subject'¹. Also, data concerning legal entities are no longer considered as 'personal data' for the purpose of application of the Data Protection Code². Likewise, legal entities are no longer considered as 'data subjects' under the Code³.

The above amendments aim to reduce the administrative burdens for data controllers for processing personal data. However, after the Decree, uncertainty arose on whether legal entities have been excluded in toto from the protection afforded by the Code.

By Resolution of 20 September 2012, the Italian Data Protection Authority (the Garante) gave an official interpretation of the amendments, clarifying that legal entities are still included into the definition of 'subscriber',⁴ thus the provisions set by the Code for the latter, in particular those included in Title X of the Code, transposing the e-Privacy Directive, still apply to legal entities.

In particular, legal entities may still benefit from the protection afforded by Section 130 of the Data Protection Code to 'subscribers' against unsolicited marketing, whereby:

- use of automated calling or communications systems for the purposes of direct marketing or sending advertising materials, or for carrying out market

dataprotectionlaw&policy

surveys or interactive business communication, as well as electronic communications by email, fax, MMS or SMS or other means for the same purposes, requires subscriber's or user's consent;

- companies may contact any subscriber whose number is published in public telephone directories for telemarketing purposes, unless the subscriber has registered its wish not to be contacted into the Italian telephone opt-out register (Registro delle Opposizioni)⁵. The opt-out principle applies only to the processing of personal data in directories by means of non-automated calls or direct mailing for the purpose of sending advertising materials, performing direct selling activities or conducting market surveys or promotional communications campaigns.

Therefore, from a practical standpoint, companies, associations or corporate bodies cannot be contacted if they have denied their consent or if they have registered in the opt-out register.

Cookies

With the long-awaited Legislative Decree No. 69/2012 of 28 May, 2012, after almost a year of delay, Italy implemented the EU e-Privacy Directive no. 2009/136/EC, which amended Directive 2002/58/EC, providing for an 'opt-in' principle to use cookies.

In particular:

- storing information on users' computer equipment 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 Garante;
- consent can be expressed through the settings of a software or other devices⁶.

Consent from users shall not be obtained for 'technical' cookies, i.e. cookies used for the sole purpose of carrying out the transmission of a communication over an electronic communications network, or strictly necessary for the provision of an information society service (which has been explicitly requested by the user). Information notice shall be in any case provided to users.

In particular, according to the Article 29 Working Party's recent opinion (WP194), users' prior informed consent is not required for session-ID cookies (e.g. shopping cart session cookies); authentication cookies and multimedia player cookies (e.g. FlashPlayer cookies); if they expire at the end of each session; customisation cookies (e.g. language preference cookies); or social network content sharing cookies for users who are 'logged in' to the relevant social network⁷.

dataprotectionlaw&policy

However, cookies used for profiling and marketing purposes may only be placed on users' computer equipment if prior informed consent is obtained, in compliance with the opt-in rule.

The above-described changes to the rules on cookies are less substantial in Italy than in the rest of Europe.

Indeed, the opt-in rule was actually already provided by the Italian Data Protection Code, even though it only applied to technical cookies, whilst any other type of unauthorised access or storage in the user's PC was prohibited. This rule, however, has never been enforced by the Garante and the opt-out through the user's browser settings has been (and still is) a common practice.

The opt-in rule for the use of cookies by website operators has stirred a controversy about how to implement it. The Garante launched a public consultation to gather proposals from consumers and operators and lay down appropriate user information mechanisms. The public consultation, which opened on 19 December 2012, will close on 19 March 2013.

Data breach notification

Legislative Decree No. 69/2012 required providers of publicly available electronic communications services (e.g., telecom operators, internet access providers) to deal with personal data breaches.

Under the new provisions, providers shall notify the Garante of the personal data breach without undue delay. In most serious cases, providers shall also report breaches to the subscriber or other individuals without delay.

On 26 July 2012, the Garante issued guidelines and instructions for the implementation of the new security requirements in connection with, in particular:

- the circumstances under which a provider shall be obliged to notify personal data breaches;
- the format of the notification;
- the manner in which the notification is to be made.

Furthermore, the Garante consulted on certain topics which are relevant for purposes of implementation of the new requirements in order to harmonise procedures and modalities of notification of personal data breaches, however the outcome of the consultation has not been published yet.

dataprotectionlaw&policy

Security measures

A recent Decree No. 5/2012, ratified by Law of 4 April 2012, No. 35, simplified the security obligations imposed on data controllers by the Italian Data Protection Code.

In particular, the Decree abolished the obligations for data controllers electronically processing sensitive data and judicial data to draft and update a security policy document (Documento Programmatico sulla Sicurezza). This document had to describe the relevant data processing operations and the security measures. In addition, the adoption and any significant change of the security policy document were to be referred to in the minutes of a Board of Directors' meeting.

Nonetheless, the other security measures prescribed by the Italian Data Protection Code remain in place, for example computerised authentication, such as username and passwords, use of authorisation systems, implementation of back-up and restoration procedures for safeguarding data and systems, and others.

Key trends for 2013

Doubts arise on whether the changes to the Italian data protection framework over the last year really succeeded in reducing the administrative burdens for enterprises processing personal data. Due to the several amendments to the Data Protection Code, the overall framework has become more uncertain. In 2013, there will be a new government in Italy, and it is highly desirable that it will move toward a more comprehensive approach to data protection. New guidance for cookies and data breaches is expected to come out in 2013. Further, the growing use of mobile devices, apps, cloud computing technologies and big data are likely to be some of the key trends over the next 12 months.

Laura Liguori

Partner

Portolano Cavallo Studio Legale

lliguori@portolano.it

Federica De Santis

Associate

Portolano Cavallo Studio Legale

fdesantis@portolano.it

Footnotes:

1. Section 40, paragraph 2, of Decree no. 201/2011.

2. According to Section 4, paragraph 1, letter b), of the Data Protection Code, personal data are 'any information relating to natural persons that are or can be identified, even indirectly, by reference to any other information including a personal identification number.'

3. Amended Section 4, paragraph 1, letter i), of the Data Protection Code considers data subject as 'any natural person that is the subject of the personal data.'

dataprotectionlaw&policy

4. According to Section 4, paragraph 2, letter f), of the Data Protection Code, 'subscriber' shall mean 'any natural or legal person, body or association who or which is party to a contract with the provider of publicly available electronic communications services for the supply of such services, or is anyhow the recipient of such services by means of pre-paid cards.'

5. Sections 129, paragraph 1, and 130, paragraph 3-bis, of the Data Protection Code. The register, which entered into force on 31 January 2011, lists the details of subscribers who do not want their numbers to be used for telemarketing purposes.

6. Section 122 of the Data Protection Code.

7. Opinion no. 4/2012.

dataprotectionlaw&policy