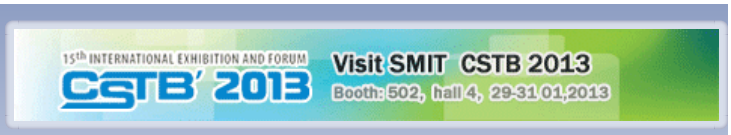




# Developments in data protection in 2012 and trends for 2013

2012 was a very busy year for Italian law-makers. Several laws significantly amended the Italian data protection legal framework, as set forth in the Italian Data Protection Code (Legislative Decree No 196/2003).

It is, however, questionable whether these changes genuinely succeeded in achieving their main objective: to reduce the administrative burdens on enterprises processing personal data. Furthermore, the various amendments to the Data Protection Code made the overall framework even less clear.

Here follows a selection of the most relevant innovations in the Italian data protection legal framework and a preview of the trends for 2013.

**REVIEW OF 2012**

**• New definition of personal data and data subject**
In December 2011 the Italian Government passed Decree No 201/2011, which excluded legal entities from the definitions of "data subject" and "personal data".

These amendments were aimed at reducing the bureaucratic requirements and administrative burdens on data controllers processing personal data. However, uncertainty arose as to whether legal entities had been excluded in toto from the protection afforded by the Data Protection Code.

With its Resolution of 20 September 2012 the Italian Data Protection Authority (Garante) gave an official interpretation of the aforementioned amendments, clarifying that legal entities were still included in the definition of "subscribers", and that the provisions set forth by the Data Protection Code for the latter (e.g. unsolicited marketing communications and telemarketing rules) therefore still apply to them.

**• Cookies**
With the long-awaited Legislative Decree No 69/2012, after almost a year of delay, Italy implemented EU e-Privacy Directive No 2009/136/EC, which amended Directive 2002/58/EC and provided for an "opt-in" principle regarding the use of cookies (i.e. small files that store information on users' computer equipment).

As a result of the implementation of the e-Privacy Directive:

− 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 issued by the Garante.

− Consent can be expressed through the settings of a piece of software or other device.

User consent is not always required. In line with the guidance provided by the Article 29 Data Protection Working Party, users' prior consent shall not be obtained for technical cookies such as: session-ID cookies (e.g. shopping cart session cookies used for purchasing items online); authentication cookies and multimedia player cookies (e.g. Flash Player cookies), provided they expire at the end of each session; customization cookies (e.g. language preference cookies) or social network content sharing cookies for users who are "logged in" to the relevant social network.

Information shall in any case be provided to users, although consent need not be obtained.

As regards the information requirement, with Resolution of 22 November 2012 the Garante launched a public consultation among consumers and the main relevant operators to gather proposals and lay down appropriate user information mechanisms. The public consultation, which opened on 19 December 2012, will close on 19 March 2013.

**• New data breach notification requirements**
Legislative Decree No 69/2012 required providers of publicly available electronic communications services (e.g. telecoms operators and Internet access providers) to deal with personal data breaches (i.e. breaches of security leading to the accidental destruction, loss, or unauthorized disclosure of, or access to, personal data processed in connection with the provision of a publicly available electronic communications service).

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

On 26 July 2012, the Garante issued guidelines and instructions for the implementation of the new security requirements in specific connection with the circumstances in which a provider shall be obliged to notify of personal data breaches, the format of the notification and the manner in which the notification shall be made.

Furthermore, the Garante launched a public consultation on certain topics related to the implementation of the new requirements in order to

harmonize the procedures and modalities of the notification of personal data breaches.

While the public consultation is closed, its outcome has not yet been published.

**• Security measures**
A recent Decree (No 5/2012) simplified the security obligations imposed on data controllers.

In particular, the Decree abolished the obligations of those processing sensitive data (e.g. data disclosing racial or ethnic origin, sexual orientation or health) or judicial data (e.g. data disclosing convictions for criminal offences) by electronic means to draft and update a security policy document ("Documento Programmatico sulla Sicurezza") by 31 March of each year.

This document shall include, amongst other content, a description of the relevant data processing operations carried out and the security measures implemented. In addition, the adoption of, and any significant update to, the security policy document shall be referred to in the minutes of a board of directors' meeting.

Nonetheless, the other security measures prescribed by the Data Protection Code remain in place (e.g. computerized authentication, such as usernames and passwords, the use of authorization systems, and the implementation of back-up and restoration procedures for safeguarding data and systems).

**• The processing of judicial data**
Decree No 5/2012 extended the possibility of data controllers processing judicial data. Before the Decree, the processing of judicial data was only allowed where authorized by either a specific statutory provision or by the Garante, specifying a substantial public interest justification, the categories of the processed data and the operations that may be performed on the data.

The Decree introduced the additional possibility of processing judicial data in accordance with agreements to prevent and counter organized crime entered into with the Ministry for Home Affairs and/or its peripheral offices. Such agreements shall specify the categories of processed data and the processing operations to be performed.

**PREVIEW OF 2013**
In 2013 there will be a new Government in Italy, which will hopefully move towards a more comprehensive approach to data protection. Here follows a preview of the top privacy trends for 2013.

**• Cookies**
Recent 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. Any other type of unauthorized access or storage in the user's PC was prohibited.

This rule, however, had never been enforced by the Garante and an opt-out through the user's browser settings had been (and still is) common practice.

The opt-in rule for the use of cookies by website operators has stirred controversy about how to implement it from a practical standpoint.

Will the Garante's new guidance on cookies help website operators to deal with the "opt-in" rule?

**• Data breaches**
2013 should be the year that more companies embrace the concept of security breaches within the context of their broader IT strategy in order to deal with security vulnerabilities.

Security on mobile devices should also be a major issue in 2013.

Guidance from the Garante is expected based on the recently closed public consultation.

**• Mobile advertising**
As the use of mobile devices and apps grows, tracking and profiling technologies will pose increasing risks to users' online privacy and new challenges for the online/mobile business.

**• Privacy by design and privacy by default**
Mobile devices pose privacy challenges that are unique to the mobile context. Specifically, controllers and app developers will increasingly consider privacy issues from the very outset of the design process, under a 'privacy by design and privacy by default' approach.

This approach will also characterize the development of any product or software involving the processing of personal data.

**• Cloud computing**
The ever-expanding adoption of cloud computing technologies by companies will raise significant issues, mainly surrounding a lack of control over personal data and questions about how, where and by whom personal data is processed.

**• Binding corporate rules (BCR)**
BCR are internal codes of conduct that establish policies for the transference of personal data outside the EU. European Data Protection Authorities launched BCR for processors on 1 January 2013. Over the next 12 months we expect an increasing number of multinational companies to start using BCR.

**• EU Data Protection Regulation**
The Italian data protection framework is set to be shaken up by the future EU Data Protection Regulation, proposed by the European Commission on 25 January 2012, which aims to reform data protection laws across the EU. The proposal is currently under scrutiny at EU level. Once it is formally adopted, the Regulation will be directly applicable to all Member States and businesses will have a two-year timetable to become compliant with the new obligations. Companies may wish to start considering the new requirements now in order to be well prepared once the Regulation enters into force.

RAPIDTVNews media smart business ready © 2013 Rapid TV News Terms of Use Privacy Policy