PORTOLANO CAVALLO
studio legale

Guidelines From the Italian Data Protection Authority on Personal Data Breaches in the Electronic Communications Sector

October 8, 2012

By Laura Liguori and Federica De Santis

Introduction

By virtue of the implementation in Italy of the e-Privacy Directive 2009/136/EC (which amended Directive 2002/58/EC) ("**e-Privacy Directive**") on May 28, 2012,i providers of publicly available electronic communications services are now subject to strict requirements to deal with personal data breaches.

In line with the e-Privacy Directive, the Italian Data Protection Code (Legislative Decree of June 30, 2003, no. 196) considers "personal data breach" to be a breach of security that leads 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.ii

According to the new provisions, the provider of a publicly available electronic communications service shall take technical and organizational measures that are adequate in the light of the existing risk.iii

Providers shall notify the Italian Data Protection Authority ("**DPA**") of the personal data breach without undue delay. In more serious cases, providers shall also report breaches to the contractor or other individuals without delay.iv

On July 26, 2012, the Italian DPA issued guidelines and instructions for the implementation of the new security requirements ("**Guidelines**") 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.v

Furthermore, the Italian DPA launched a public consultation on certain topics which are relevant for purposes of implementation of the new requirements in order to harmonize procedures and modalities of notification of personal data breaches and to "*collect from TLC companies and ISPs useful elements to assess the adequacy of the new measures.*"vi

The public consultation will be closed within 90 days of the publication of the Guidelines.

Scope of Application of the Notification Duty

The Guidelines clarify that the notification duty applies only to "providers of publicly available electronic communications services", *i.e.* to subjects providing, via public communications networks, services which consist wholly or mainly in the conveyance of signals on electronic communications networks (*e.g.,* telecom operators, Internet access providers).vii

Therefore, in line with the e-Privacy Directive, the new requirements do not apply to all data controllers. In particular, according to the Guidelines, the following operators shall not be subject to the new requirements:

- providers of electronic communications services to a small group of persons (e.g. employees or collaborators of the provider);
- owners of public or private businesses who make available to the public, clients or partners terminal devices for communications or wireless Internet access points;
- Internet content providers;
- search engines operators.

Moreover, the new requirements apply only in connection with the provision of the abovementioned electronic communications services. Therefore, if the data breach concerns a database of the provider which is not specifically linked to the service offered by the same, but is instead used for a different purpose (e.g., management of the employment relationship or accountancy), the new requirements would not apply.

That being said, the Italian DPA acknowledged that the proposal for EU data protection regulation issued by the EU Commission on January 25, 2012 provides for data breach requirements in relation to any data controllers on grounds that the interests of users in being notified is not limited to the electronic communications sector.viii

The opportunity to apply the data breach notifications requirements to all data controllers has been stressed also by the Article 29 Data Protection Working Partyix 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, it is worth noting that in May 2011 the Italian DPA applied the notification duty to operators other than providers of publicly available communications services, as it required banks to promptly notify the Italian DPA about any data breach which led to the destruction, loss, modification and/or unauthorized disclosure of customers' personal data, as long as said breach is large enough, either in terms of the quantity or quality of data involved in the breach or the number of subjects affected by it, to warrant a notification duty.x

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 abovementioned notification requirements.

All data controllers, even if not subject to the new provisions to data breach notification requirements, must in any case implement the minimum security measures as set forth by the Data Protection Code

and its Annex B (e.g., computerized authentication, such as username and password, use of authorization systems, use of anti-virus software, etc.)xi

Risk Assessment

According to the Guidelines, the first step to comply with the new security requirements is to carry out a risk assessment, including the relevant thresholds (*e.g.,* low, medium, high) which should guide the provider in the selection of the most adequate measures to address the breach.

Adoption of Adequate Measures (Under Public Consultation)

Pursuant to Section 32 of the Data Protection Code, providers must adopt technical and organizational measures that are adequate in light of the existing risk.

The Guidelines identify the following measures as adequate:

- making personal data no longer available for further data processing operations, by means of erasure or anonymization of said data;
- implementation of measures to control the activities carried out on the personal data by each person in charge of the processing;
- paying special attention to hand-held devices, with a view to ensure a level of security at least equal to the one applied to other devices on the grounds that data breaches often involve hand-held devices used by employees and collaborators outside the provider's premises.

It is expected that the contributions to the public consultation will suggest further measures that meet the adequacy requirement.

Notification of the Italian DPA

Neither the e-Privacy Directive nor the Data Protection Code specify when a notification of a data breach is due, it provides only that a notification should be made "without undue delay".xii

The Guidelines clarify that, within 24 hours from acknowledgment of a data breach, providers must provide to the Italian DPA preliminary information including, at least:

- the identification data of the provider;
- a brief description of the data breach;
- the date, even presumptive, when the data breach occurred;
- the place where the data breach occurred;
- a description of the nature and content of the concerned data;
- a brief description of the systems used for the elaboration and storing of the concerned data, including their location.

Within the following 3 days, providers must forward to the Italian DPA more detailed information, including, among others: the consequences of the data breach and the measures proposed or taken to address the same.

Notifications may be carried out by using a form available via the Italian DPA's website. Other modalities of notification are currently under examination.

Inventory of Personal Data Breaches

Providers shall keep an updated 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.xiii

Notification to Contractors or Other Individuals (Partly Under Public Consultation)

According to the Guidelines, notification to the contractor or other individuals whose data were affected by a breach (which is due only in case of the most serious breaches, i.e., if the breach is likely to adversely affect the personal data or privacy of a contractor or another individual) must be made within 3 days from acknowledgment of the data breach. However, breaches concerning authentication credentials (e.g., username and password) warrant immediate notification.

Notification is not required if the provider is able to give evidence to the Italian 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 affected by the security breach.xiv

The Guidelines provide some examples of circumstances where personal data could be considered to be unintelligible (thus, notification to the contractor or other individual is not in principle due):

- data ciphered by means of a standardized algorithm;
- data replaced with an hash value using cryptographic technologies;
- data anonymized in such a way to make it impossible to identify data subjects.

This specific topic is currently under public consultation, thus it is expected that operators will provide the DPA with other examples of circumstances and technologies that would make data unintelligible.

In any case, if the provider has not already notified the contractor or other individuals of the personal data breach, the DPA may require it to do so having considered the likely adverse effects of the breach, regardless of the fact that data have been made unintelligible.

Where breaches involve a large number of persons, far-reaching/public communications (e.g., on newspapers, radio, etc.) should be preferred over individual forms of notification.

The public consultation should also provide examples of data breaches that could trigger notification to the contractor or other individual which, as clarified, is due solely if the breach is likely to adversely affect the personal data or privacy of said subjects.

According to the Guidelines, the assessment concerning the decision to report breaches to contractors or other individuals should take into account:

- the prejudice that loss or destruction of data could result in (e.g. identity fraud, reputational damage, etc.);

- whether the personal data breached are still relevant (recent data can be more valuable to infringers);

- the quality of personal data (e.g., whether a breach involves sensitive or judicial data) and the amount of data involved in the breach (e.g., breaches involving only one personal data, or non-sensitive personal data could be exempted from notification).

The goal of the public consultation on this topic is basically to identify common criteria among the providers for the evaluation concerning the kind of cases requiring notification to contractors or other individuals.

Sanctions

Failure or delay to notify a personal data breach to the Italian 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 for each contractor or individual.[xv]

Providers' failure to keep an inventory of personal data breaches can be sanctioned with a fine ranging between EUR20,000 to EUR120,000.[xvi]

Provision of untrue information, or submission of untrue records or documents, in connection with the notification to the Italian DPA in the case of data breaches, is punished with imprisonment from six months to three years.

First published on: Rapidtvnews.

[i] Legislative Decree of May 28, 2012, no. 69, which entered into force on June 1, 2012.

[ii] Section 4, paragraph 3, letter g-bis), of the Data Protection Code.

[iii] Section 32, paragraph 1, of the Data Protection Code.

[iv] Section 32-bis, paragraphs 1 and 2, of the Data Protection Code.

[v] Pursuant to new Section 32-bis, paragraph 6, of the Data Protection Code, the Italian DPA may issue a decision containing guidelines and instructions with regard to the circumstances under which a provider is obliged to notify personal data breaches, the format of such notification, and the manner in which the notification is to be made.

[vi] Press release published on the Italian DPA's website on August 1, 2012.

[vii] Definitions of "public communications network" and "electronic communications service" are provided by Section 4, paragraph 2, letters d) and e), of the Data Protection Code.

[viii] See also Recital 59 of the e-Privacy Directive: "*(...) explicit, mandatory notification requirements applicable to all sectors should be introduced at Community level as a matter of priority*".

[ix] Opinion no. 1/2011 of April 5, 2011, on the current EU personal data breach framework and recommendations for future policy developments.

[x] Italian DPA's Resolution of May 12, 2011.

[xi] Section 34 of the Data Protection Code; Annex B to the Italian Data Protection Code.

[xii] Section 4, paragraph 3, of the e-Privacy Directive; Section 32-bis, paragraphs 1, of the Data Protection Code.

[xiii] Section 32-bis, paragraph 7, of the Data Protection Code.

[xiv] Section 32-bis, paragraph 3, of the Data Protection Code.

[xv] Section 162-ter, paragraphs 1 and 2, of the Data Protection Code.

[xvi] Section 162-ter, paragraph 4, of the Data Protection Code.