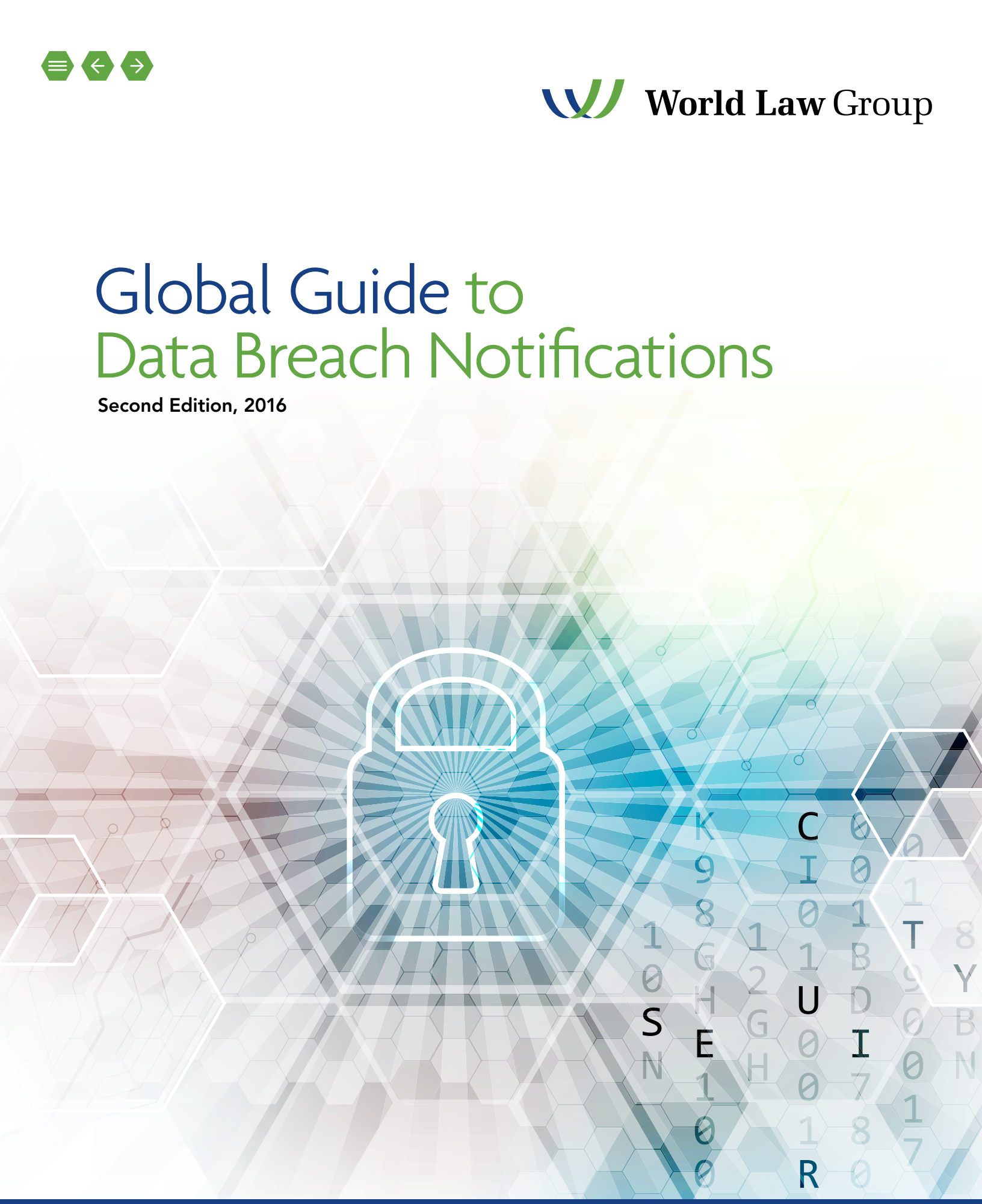
World Law Group

Global Guide to Data Breach Notifications

Second Edition, 2016



globaldatabreachguide.com

28. ITALY[23]

28.1 In the event of a data breach affecting residents of your country, is there any legal obligation or requirement to notify either a) affected individuals; or b) a regulator such as a data protection authority (DPA)?

Yes, but only for:

- Banks and financial institutions;
- Public electronic communications providers;
- Data controllers processing biometric data;
- Distinct health data controllers sharing among each other electronic information and health data originated from individuals' clinical history, by means of the "Electronic Health File"; and
- Health professionals operating within a data controller and sharing health information summarizing the health history of an individual by means of the "Electronic Health Dossier".

28.2 Under what conditions must such notification(s) be given, including a) what types of data must be breached to trigger notification; and b) whether the entity must be a data controller or data processor in your country for such obligations to apply?

Regarding banks and financial institutions, notification must be given for any data breach involving a bank's customers' data. Regarding public electronic communication providers, notification is required for any breach of personal data involved in the providing of the communication services. In relation to data controllers processing biometric data, notification is required for any data breach and/or IT incident that may significantly impact biometric systems or the data stored, even though it does not impact them directly.

In relation to the "Electronic Health File," notification is required for any IT attack, fire and/or other incident able to cause the loss, destruction or the unauthorised dissemination of the data. In relation to the "Electronic Health Dossier," notification is required for any data breach and/or IT incident that may significantly impact the respective health data, even in case of indirect impact.

In all cases above, the notification obligation is only on the controller.

[23] Italy is a member state of the European Union. If you are interested in the EU law requirements, please refer to the section on the European Union.

28.3 For such notification(s), is there any required or suggested a) content of the notice; b) time period in which notice must be given; or c) method of giving notice, such as regular mail, email, web-posting or publication?

In relation to the obligation of notification by banks and financial institutions, the provision requires a detailed notice which must be given promptly.

In relation to the notification imposed on public electronic communication providers, the notice shall contain a brief description of the personal data breach, the nature of the personal data and information systems involved, the actual effects and possible consequences of the breach, as well as the security measures adopted and to be adopted by the electronic communications provider to impede or reduce such events. The notice must be given without undue delay.

In 2013, the Italian DPA, following a public consultation on data breach notification in the electronic communication field in 2012, issued a provision setting out specific guidelines on the matter. This provision proposes a time limit of 24 hours for a first brief notice and three days for a further detailed notice, and provides for an ad hoc notification form (available online via the DPA's website) to gather information on data breaches in a way that allows this information to be processed electronically by the DPA.

In relation to data controllers processing biometric data, the notice shall indicate the nature and kind of the data breach, a brief description, the information systems involved, the categories of the data and the number of data subjects affected, as well as the security measures adopted and to be adopted to prevent or contain such events. The notice shall be made within 24 hours from the time the data controller becomes aware of the event, and in accordance with the specific template provided by the DPA on its website.

In relation to the Electronic Health File, the notice shall describe the data breach, including the categories and number of data subjects involved, the contact of the data protection officer or other person in charge, the description of the consequences of the data breach, as well as the measures proposed or adopted to remedy the violation. The notice shall be sent within one week of the event.

Regarding the Electronic Health Dossier, the notice shall contain a brief description of the data breach, the nature of the data breach and data affected, the information systems and/or devices involved, as well as the number of data subjects and the security measures adopted and to be adopted to prevent or minimize such events. The notice shall be sent to the DPA, in the form of the specific template provided by its website, within 48 hours of first knowledge of the event. Furthermore, the data controller shall internally adopt a procedure to give to the data subject, without undue delay, notice of the data breach.

28.4 What are the penalties, fines or risks in failing to notify, either by the DPA or in litigation?

Failing to notify can result in a fine and strict liability in tort action.

28.5 Even if there is no current legal obligation to do so, or if there is no "data controller" or "data processor" located in your country, is notification to individuals recommended in the event of a data breach affecting residents in your country (such as in credit card data breaches)?

In general, notification is recommended even when it is not mandatory. This determination should be made on a case-by-case basis.

28.6 What are the applicable data protection laws or guidelines within your country?

The main data protection national laws and regulations are:

- Legislative Decree 196/2003 "Personal Data Protection Code";
- "Provisions in the matter of flows of banking information and tracking of banking operations" of 12 May 2011;
- "Guidelines in the matter of implementation of the provisions on data breach notifications – Public consultation" of 26 July 2012;
- "Implementing measures with regard to the notification of personal data breaches" of 4 April 2013;
- "General Application Order Concerning Biometrics" of 12 November 2014;
- "Opinion on the draft of Decree of the President of the Council of Ministers in matter of Electronic Health File" of 22 May 2014; and
- "Guidelines in matter of Electronic Health Dossier" of 4 June 2015.

28.7 Contact information for Data Protection Authority:

Name:	Garante per la protezione dei dati personali
Address:	Piazza di Monte Citorio n. 121, 00186 Roma, Italy
Telephone:	+39 06 6967 71
Fax:	+39 06 6967 73785
Email:	garante@gpdp.it
Website:	www.garanteprivacy.it

For more information, contact:

Name:	Daniele Vecchi
Firm:	Gianni, Origoni, Grippo, Cappelli & Partners
Address:	Piazza Belgioioso, 2 20121, Milan, Italy
Telephone:	+39 02 7637 41
Fax:	+39 02 7600 9628
Email:	dvecchi@gop.it
Website:	www.gop.it