World Law Group

Global Guide to Data Breach Notifications, 2013

Review Proof

World Law Group
Global Guide to
Data Breach Notifications

Please note that this guide provides general information only. Its purpose is to provide a brief overview of legislation governing data breach notification requirements in each jurisdiction covered. This information is not comprehensive and is not intended as professional or legal advice, generally or in a given situation. This guide is an outline of country-specific obligations, which may change. Facts and issues vary by case. Local legal counsel and advice should routinely be obtained. For additional information or advice in a particular jurisdiction, you may contact the members of the World Law Group's Privacy Matters Practice Group as listed in the "Contacts" section.

Review Proof

CONTENTS

Review Proof

INTRODUCTION

Management of a data breach is a complex task, whether localised or spanning different countries. Organisations need to react nimbly and quickly to navigate the dense fabric of security breach notification requirements of various locations and jurisdictions.

In recent years, there have been an increasing number of well-publicised breaches in all business sectors, and numerous studies confirm that data breaches present a costly and significant exposure to companies, both monetary and reputational. Fines, penalties and litigation that can result from violations present an increasing exposure, which sometimes can be minimised by a rapid, thoughtful and well-organised response to a breach.

There is a growing body of regulations and statutes that govern companies' collection and use of information about individuals, and the disclosures they are required to make. Many of those laws focus on the types of personal information that are often the subject of data breaches — and a target for those seeking to engage in identity theft and use such information for fraudulent financial transactions.

These obligations are no longer limited to one country's laws. For example, a malware intrusion, in which the hackers are able to export credit card information to an off-shore website, may compromise data about residents of a number of countries. Also, different systems or databases at a company may be attacked in various locations.

Compliance with this growing body of law now requires becoming familiar with and addressing the variations in national law. Even identifying those laws can be a challenge for the most experienced practitioners, privacy or compliance officers and risk management executives. Because personal data breach reporting requirements around the world are, at present and for the foreseeable future, a mismatched patchwork, this challenge is further magnified.

This is true both in the U.S., with its multiplicity of privacy and breach notification laws, and within Europe, where the requirements stem from common European directives. Other countries are also instituting their own data breach reporting rules. In many countries, as reflected in this guide, there are often recommendations to report the breach to individuals or data authorities, even when the laws do not explicitly require it.

Accordingly, the aim of this publication is to distil the experience of privacy and data protection lawyers from numerous World Law Group member firms into a single reference to help with this complex navigation exercise.

This guide focuses on the patchwork of laws around the world as they currently stand at the date of publication. But change in this area is constant. Please visit www.globaldatabreachguide.com where we expect to post updates as they become available.

Expected European Changes

In the future, personal data security breach laws in Europe will likely be harmonised. The draft EU Data Protection Regulation will replace the current European Data Protection Directive (and implementing national laws) and will likely not come into force until 2016 but there is a chance this date could be brought forward. The personal data breach notification requirements will probably be stringent and penalties for non-compliance even more so (amounting to as much as 2% of global annual turnover). The proposed Regulations will require mandatory notification of breaches to regulators within a very short time, perhaps 24-72 hours, and notification is to be accompanied by a raft of information.

At the same time, Europe is in the process of extending cyber-security requirements to a range of information service providers which will also include mandatory breach notification requirements.

Acknowledgments

This guide would not have been possible without the extraordinary contributions of lawyers from Wragge & Co LLP in the UK. Kirsten Whitfield, a Director with Wragge & Co, along with Amelia Angus and Mike Reed, both trainee solicitors at that firm, worked tirelessly to organize, edit and otherwise facilitate the production of this guide. The WLG Privacy Matters Group is exceedingly grateful for the fine efforts and determination of Wragge & Co in helping see this project through to conclusion.

Mark E Schreiber, Chair, WLG Privacy Matters Group, Edwards Wildman Palmer LLP, Boston

Christian Runte, Co-Chair, WLG Privacy Matters, CMS Hasche Sigle, Munich

ABOUT WORLD LAW GROUP

The World Law Group (WLG) is a network of 51 leading independent law firms with more than 300 offices in major commercial centres worldwide. WLG member firms comprise more than 16,000 lawyers working in a comprehensive range of practice and industry specialties. Clients can access local knowledge, and seamless multinational service via a single call to any WLG member firm.

A full list of all member firms of the World Law Group and their respective contact partners is available at www.theworldlawgroup.com. If jurisdictions relevant to your organisation are not included in this guide, WLG members can usually provide contacts for those purposes.

For more information, visit www.theworldlawgroup.com.

About the WLG Privacy Matters Group

The World Law Group's Privacy Matters Practice Group is made up of lawyers in the WLG's member firms worldwide who have data protection, privacy and related compliance work as a focus of their practice, both in their countries and globally. The group's goal is to enhance the provision of relevant and seamless client services, including cross-border data transfers, privacy risk assessment and data breach services to multinational entities, and to develop proactive compliance procedures and techniques in this increasingly demanding field.

Group members from around the world meet by teleconference and at many WLG semi-annual conferences to exchange information about emerging privacy issues and challenges for multinational and local country clients, and to work together on various projects. Group members have collaborated on several noteworthy publications both online and in print and have organised numerous webinars and other information events for members and clients.

Members have collaborated to produce, for example, the WLG's Global Guide to Whistleblowing Programs (May 2012) and a seminal chapter on "Anonymous Sarbanes-Oxley Hotlines for Multinational Companies: Compliance with E.U. Data Protection Laws", for the American Bar Association's *The Practitioner's Guide to the Sarbanes-Oxley Act*, (2009).

For more information, contact:

Mark E. Schreiber
Chair, WLG Privacy Matters Group
Edwards Wildman Palmer LLP
Boston, Massachusetts, U.S.A.
Email: mschreiber@edwardswildman.com
Tel: + 1 617 239 0585

Christian Runte
Co-Chair, WLG Privacy Matters Group
CMS Hasche Sigle
Munich, Germany
Email: christian.runte@cms-hs.com
Tel: + 49 89 238 070

ARGENTINA

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)?**

   There is no specific legal obligation or requirement under Argentine law to notify either affected individuals or the DPA (the *Dirección Nacional de Protección de Datos Personales*) of a data breach. However, the data controller must keep a register of security incidents, where any data incident it becomes aware of must be recorded.

   Note that the DPA, under Disposition No. 11/2006, established three levels of security measures according to the nature of personal data processed, providing different security measures to be adopted according to the level of security applicable to the data. The DPA is entitled to verify the compliance of data security rules, to conduct investigations and to request information, documents and any other element related to treatment of personal data (i.e. the security incidents register), that the DPA considers necessary.

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?**

   Not applicable.

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?**

   Not applicable.

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

   Not applicable.

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)?**

   Each event should be analyzed on a case by case basis when deciding whether to notify an individual of a data breach. Key points of consideration include the risk of dissemination,

scope of data involved, magnitude of damage, measures that may be adopted by the individual to prevent the dissemination or prevent damages and chance of obtaining non-disclosure injunctions.

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

The main data protection national laws and regulations are the following:

- Section 43 of the Constitution of the Argentine Republic provides a special court remedy called "*habeas data*" for the protection of personal data, which upgrades the protection of personal data to the category of a fundamental right;
- Law No. 25,326 (the "Personal Data Protection Law") and its Regulatory Decree No. 1558/2001 contain, among other provisions: general data protection principles, the rights of data subjects, the obligations of data controllers and data users, the rules for transfer of personal data, the creation of the controlling authority, penalties for the event of breach and rules of procedure for the "habeas data" court remedy;
- According to Section 9, both the persons in charge of a database and its users must adopt such technical and organisational measures as may be necessary to guarantee the security and confidentiality of personal data, in order to avoid a data breach. In addition, storing personal data in files, registers or banks that do not meet technical integrity and security requirements is forbidden; and
- Criminal Code, Sections 117 bis and 157 bis address crimes regarding personal data violations and impose prison sentences for persons committing those crimes.

In addition there are a number of dispositions issued by the *Dirección Nacional de Protección de Datos Personales*, including:

- Disposition No. 2/2005, which created the National Registry of Databases and provides for the compulsory registration of certain databases with such Registry;
- Disposition No. 7/2005, which provides a classification of infringements and graduation of the penalties for violation of the Personal Data Protection Law and its ancillary regulations;
- Disposition No. 11/2006 and Disposition No. 9/2008, which specify security measures for the treatment and conservation of personal data stored in databases;
- Disposition No. 10/2008, which specifies information that must be provided on websites, forms of communication, advertisements and in forms used to collect personal data; and
- Disposition No. 4/2009, which sets out direct marketing-related obligations.

7. Contact information for Data Protection Authority:

Name:	Dirección Nacional de Protección de Datos Personales
Address:	Sarmiento 1118, Floor 5°, Buenos Aires City, Argentina, C1041AAX
Telephone:	+54 11 4383 8512
Email:	Email enquiry available via website
Website:	www.jus.gov.ar/datos-personales.aspx

For more information, contact:

Name:	Carlos E. Alfaro or Giselle Geuna
Firm:	Alfaro-Abogados
Address:	Avenida Del Libertador 498, Floor 3°, Buenos Aires, Argentina
Telephone:	+54 11 4393 3003
Fax:	+54 11 4393 3001
Email:	calfaro@alfarolaw.com or ggeuna@alfarolaw.com
Website:	www.alfarolaw.com

AUSTRALIA

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)?**

   There is no legal obligation or requirement under Australian law to notify either affected individuals or the DPA (the Office of the Australian Information Commissioner) of a data breach.

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?**

   Not applicable.

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?**

   Not applicable.

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

   Not applicable.

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)?**

   The Privacy Commissioner has issued guidelines which recommend that relevant individuals and the Privacy Commissioner be notified where there is a risk of serious harm occurring as a result of the breach.

   In late 2012, the Federal Government released a Discussion Paper on mandatory data breach notification laws. While it is unlikely that the proposal will advance further until after the Federal election in September 2013, it is very likely that mandatory data breach notification provisions will soon become part of Australian privacy legislation.

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

The key legislation is the Federal Privacy Act (Cth) 1988.

The Privacy Amendment (Enhancing Privacy Protection) Act (Cth) 2012 will come into force from March 2014. At this stage, the new legislation will not change Australia's data breach notification requirements.

7. Contact information for Data Protection Authority:

Name:	Office of the Australian Information Commissioner
Address:	GPO Box 2999, Canberra, ACT 2601, Australia
Telephone:	+61 2 9284 9749
Fax:	+61 2 9284 9666
Email:	enquiries@oaic.gov.au
Website:	www.oaic.gov.au

For more information, contact:

Name:	Charles Alexander or Elisabeth Koster
Firm:	Minter Ellison
Address:	Aurora Place, 88 Phillip Street, Sydney, NSW 2000, Australia
Telephone:	+61 2 9921 4826 or +61 2 9921 4234
Fax:	+61 2 9284 9666 or +61 2 9921 8014/8434
Email:	charles.alexander@minterellison.com or elisabeth.koster@minterellison.com
Website:	www.minterellison.com

AUSTRIA

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)?**

   Pursuant to Section 24 Paragraph 2a of the DPA 2000, the controller must immediately notify the data subject in an appropriate manner if the controller learns that data from his data application have been systematically and seriously misused and the data subject may suffer damage. This does not apply if there is only a likelihood of insignificant damage and the obligation to notify all data subjects would require a disproportionate amount of effort.

   There is no legal obligation to inform the Austrian Data Protection Authority.

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?**

   Notification must be given by the controller immediately upon the occurrence of a data breach affecting the personal data of a data subject. Personal data is any data by which the data subject may be identified.

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?**

   Notice must be given as soon as possible and immediately upon the occurrence of the data breach. There is no guidance on the content or method of giving notice.

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

   Pursuant to Section 52 Paragraph 2 (4) of the DPA 2000, a fine of up to EUR 10,000 can be imposed on the controller.

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)?**

   Not applicable.

6. **What are the applicable data protection laws or guidelines within your country?**

   The Federal Act concerning the Protection of Personal Data (DPA 2000).

7. Contact information for Data Protection Authority:

Name:	Geschäftsstelle der Datenschutzkommission
Address:	Hohenstaufengasse 3, 1010 Wien, Vienna, Austria
Telephone:	+43 1 531 15 / 202525
Fax:	+43 1 531 15 / 202690
Email:	dsk@dsk.gv.at
Website:	www.dsk.gv.at

For more information, contact:

Name:	Robert Keisler or Dr. Bernt Elsner
Firm:	CMS Reich-Rohrwig Hainz
Address:	Rechtsanwälte GmbH, Gauermanngasse 2 Vienna, 1010, Austria
Telephone:	+43 1 40443/2850 or +43 1 40443/1800
Fax:	+43 1 40443 9000
Email:	robert.keisler@cms-rrh.com or bernt.elsner@cms-rrh.com
Website:	www.cms-rrh.com

BELGIUM

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

   There is no general obligation in Belgium to notify data breaches to the affected individuals or to the regulator with the following exception.

   The Act on Electronic Communications of 13 June 2005 provides for an obligation to notify data breaches in the telecoms industry. Since the amendments to the Electronic Communications Act entered into force on 4 August 2012, the providers of public electronic communications services are obliged to notify data breaches to the Belgian Institute for Postal Services and Telecommunications immediately on the occurrence of each data breach (art. 114/1 §3 of the Act).

   If the personal data breach is likely to adversely affect the personal data or the privacy of a subscriber or an individual, the provider of public electronic communications services shall also immediately notify the subscriber or the individual concerned of the breach (art. 114/1 §3 of the Act).

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?**

   In the telecommunications industry, the providers of public electronic communications services are obliged to notify in accordance with Question 1 above in the case of a breach of the security of personal data. This breach is defined as "a breach of security that leads to the accidental or unlawful destruction, loss, alteration, non-authorized disclosure of, or access to, personal data transmitted, stored or otherwise processed in relation to the provision of a public electronic communications service in the (European Union)" (art. 2-68° of the Act).

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?**

   According to article 114/1§3 of the Electronic Communications Act, the notification to the individuals must contain the following information:
   - The nature of the personal data breach;
   - The contact points for more information; and
   - The measures that are recommended to mitigate the adverse effects of the personal data breach.

The notification to the Institute must in addition contain the following information:

- A description of the consequences of the personal data breach; and
- The measures proposed or taken by the provider of public electronic communications services to solve the personal data breach.

The notification must occur as soon as possible. The method of giving notice is not provided in the Act and posting notices on the internet or other forms of publication are not required, but e-mail and regular mail are recommended.

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

In relation to a general breach there is no general obligation to notify and therefore no penalties. With regards to the Electronic Communications Act, this legislation does not provide for penalties either.

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)?

Yes, because the civil liability of the data controller or processor will increase if it does not take all the measures that are required to keep the damage as limited as possible. Notifying the individuals or the regulators about the personal data breach is the best way to keep the damage limited.

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

The main data protection legislation is the Data Protection Act of 8 December 1992.

The Electronic Communications Act of 13 June 2005 is the key legislation in relation to the exception referred to in Question 1, above.

7. Contact information for Data Protection Authority:

Name:	Commission for the Protection of Privacy
Address:	Rue de la Presse 35, 1000 Brussels, Belgium
Telephone:	+32 (0)2 274 48 00
Fax:	+32 (0)2 274 48 35
Email:	commission@privacycommission.be
Website:	www.privacycommission.be

For more information, contact:

Name:	Tom Heremans
Firm:	CMS DeBacker
Address:	Chaussée de La Hulpe 178, B-1170 Brussels, Belgium
Telephone:	+32 2 743 69 73
Fax:	+32 2 743 69 01
Email:	tom.heremans@cms-db.com
Website:	www.cms-db.com

BOSNIA AND HERZEGOVINA

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)?**

   In the case of a data breach affecting residents of Bosnia and Herzegovina, there is no legal obligation to notify affected individuals or the Personal Data Protection Agency ("DPA").

   According to Article 30 of the Law on Protection of Personal Data ("PDPL"), an individual may (but it is not obligated to) file a complaint to the Personal Data Protection Agency of the BiH.

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?**

   If an individual believes that his/her right to the protection of personal data was breached, or that his/her data were not handled fairly, the individual has the right to object and to ask the Personal Data Protection Agency that:

   a) The controller or processor refrains from such actions and corrects the factual situation caused by these actions;

   b) The controller or processor corrects or amends personal information so that it is authentic and accurate; and/or

   c) The personal data is blocked or destroyed.

   The notification must be made by the "data subject", i.e. a natural person whose identity can be determined or identified, directly or indirectly, in particular by reference to a personal identification number or to one or more factors specific to his/her physical, physiological, mental, economic, cultural or social identity.

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?**

   The complaint must be understandable and complete. The complaint shall contain:

   - The name and surname of the complainant or the note that the complainant wants to stay anonymous;
   - The name of the controller or the data processor against who the complaint had been filed;
   - A short explanation of the complaint; and
   - Evidence and signature of the complainant, or the signature of the legal representative.

There is no specified time period in which notice must be given.

The complaint may be lodged in written form and be submitted to the Agency (the DPA), by mail, fax or email. Alternatively, the complaint may be stated orally through the minutes in the Agency or be stated by telephone with written notice following. The complainant may declare a preference to remain anonymous, but the Agency shall notify him/her that the complainant shall then not be advised on the measures undertaken to address his/her complaint.

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

   Pursuant to Article 49 of the PDPL, a fine of from €5,000 up to €50, 000 can be imposed on the controller.

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

   We would recommend notifying of a security breach.

6. **What are the applicable data protection laws or guidelines within your country?**

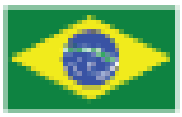
   The key legislation is the Law on Protection of Personal Data ("Official Gazette of Bosnia and Herzegovina" 49/06 and 76/11).

7. **Contact information for Data Protection Authority:**

Name:	Agencija za zaštitu ličnih podataka u Bosni i Hercegovini
Address:	Vilsonovo šetalište 10, 71 000 Sarajevo Bosnia and Herzegovina
Telephone:	+387 33 726 250
Fax:	+387 33 726 251
Email:	azlpinfo@azlp.gov.ba
Website:	www.azlp.gov.ba

For more information, contact:

Name:	Sanja Voloder
Firm:	CMS Reich-Rohrwig Hainz d.o.o.
Address:	Ul. Fra Anđela Zvizdovića 1, Sarajevo, BiH-71000, Bosnia and Herzegovina
Telephone:	+387 33 944 600
Fax:	+387 33 296 410
Email:	Sanja.Voloder@cms-rrh.com



BRAZIL

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)?**

   No. There is no data protection authority in Brazil and no laws mandating notification of data breaches to either an authority or individuals.

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?**

   Not applicable.

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?**

   Not applicable.

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

   Not applicable.

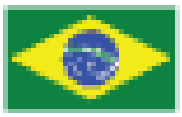
5. **Even if there is no current legal obligation to do so, or if there is no "data controller" or "data processor" located in your country, is notification to individuals recommended in the event of a data breach affecting residents in your country (such as in credit card data breaches)?**

   Yes, particularly in the case of consumer data. Although notification of security breaches is not mandatory under Brazilian law, it is highly advisable to notify individuals about security breaches, particularly if such individuals are considered consumers (i.e. end user of a product or service supplied to the individual, and the individual's data was collected in connection with such consumer relationship).

6. **What are the applicable data protection laws or guidelines within your country?**

   Unlike other countries, particularly countries within the European Union, there is neither a single privacy protection regulation nor a privacy protection agency in Brazil.

   Privacy under Brazilian law is governed by several provisions of the Federal Constitution, the Civil Code, the Consumer Defence Code and the Criminal Code. These pieces of legislation deal with different scopes of privacy, such as intimacy, private life, honour, image, secrecy of correspondence, secrecy of bank operations, secrecy of telegraphic communications, secrecy of telephone communications, and secrecy of data.



The Federal Constitution establishes that all individuals are entitled to the fundamental and inviolable rights of intimacy/privacy, private life, honour, and image, and the violation of these rights is subject to indemnification for actual financial loss and intangible harm.

The Civil Code reaffirms the Federal Constitution's fundamental rights: an individual's private life is inviolable and injured parties are entitled to take action against violators in order to stop the violation and seek compensation.

In view of the provisions of the Federal Constitution and the Civil Code, any person may file a lawsuit to recover damages resulting from unauthorized disclosure or collection of personal information or any violation of privacy rights. In these lawsuits, individuals may seek material and/or non-material damages. Indemnifications are assessed on a case-by case basis, but in general courts have been granting damages awards in cases related to negative credit information (failure in informing the individual or rectifying negative credit information in databases).

The Consumer Defence Code deals with consumer-related databases, data collection, and penalties for infringement of the corresponding provisions.

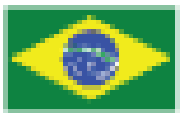
According to the Consumer Defence Code, the consumer's consent is mandatory for the collection of his/her personal data or, alternatively, the consumer must be necessarily informed, in writing, about any data collection. In case the consumer requests the inclusion of its information, no communication is necessary.

Databases of consumers must be objective, clear, and created in an easily understandable language. Consumers are entitled to access and rectify any personal or commercial information regarding them in any files, registers or records, even if the consumer has previously agreed to the collection of the relevant information. Negative credit information of consumers may only be stored for up to 5 years.

Consumers are also entitled to demand correction or update of inaccurate personal information, regardless of their previous consent for the collection of the relevant data. Any request of correction or update shall be complied with within five business days. In addition, consumers are entitled to request at any time the exclusion of their personal data from databases, provided that the relevant database is not a credit protection database.

As a general rule, Brazilian law does not require any registration or notification to competent authorities prior to collecting or processing data.

The exception to the general rule is established by the Consumer Defence Code. If the data at issue refers to consumers the consent of the consumers is mandatory for the lawful collection of data. Alternatively, the applicable law allows the collection of data if the consumer was duly informed in writing in advance and did not oppose.



In this context, if a party intends to collect data of consumers it is advisable to write a privacy notice explaining the data collection in any form, which will be presented to the consumers, either in printed or digital format.

It should be noted, however, that if the data to be collected is public, such as information collected from public databases, magazines, etc, it is not necessary to request the consent of the consumer.

There are no laws in Brazil dealing specifically with data transfer. Nevertheless, because the transfer of consumer data to third parties may be considered a new procedure for the collection of data, the comments above regarding the collection of consumer data also apply to the transfer of consumer data.

Interested parties are advised to either request the consent of consumers or communicate the intended transfer in advance, explaining its respective scope and allowing consumers to update their information.

There are no restrictions under Brazilian law dealing specifically with the international transfer of data. Nonetheless, the comments regarding the collection of data in Brazil, mentioned above, shall be taken into consideration in cases of international transfer of data, as long as such transfer represents a creation of a new database.

Therefore, in the case of international transfer of data, it is advisable to inform the owners of the personal data about such transfers, either at the moment of collection or at the moment of the actual transfer.

7. Contact information for Data Protection Authority:

Not applicable.

For more information, contact:

Name: Marcela Waksman Ejnisman or Marlio de A. N. Martins
Firm: TozziniFreire Advogados
Address: Rua Borges Lagoa, 1328, São Paulo, SP, 04038-904, Brazil
Telephone: + 55 11 5086 5000
Fax: + 55 11 5086 5555
Email: mejnisman@tozzinifreire.com.br or mmartins@tozzinifreire.com.br
Website: www.tozzinifreire.com.br

CANADA

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)?

Canada is a federal State composed of ten provinces. There is no requirement to notify the affected individuals or a data protection authority, with the exceptions of:

- The province of Alberta if required by the Privacy Commissioner of Alberta (the "Alberta Commissioner") upon receipt of a notification pursuant to the Personal Information Protection Act, S.A. 2003, c. P-6.5 ("PIPA");
- In the province of Ontario with respect to health-related personal information;
- In the province of Newfoundland and Labrador with respect to health-related personal information;
- In the province of New Brunswick with respect to health-related personal information; or
- As of June 1, 2013, in the province of Nova Scotia with respect to health-related personal information.

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?

Alberta

In Alberta, organisations that collect, use and disclose personal information about individuals must notify the Alberta Commissioner where there are losses or instances of unauthorized access to or disclosure of personal information such that a reasonable person would consider that there exists a real risk of significant harm to an individual.

The factors to be considered when determining whether a real risk of significant harm has occurred include:

- The number of affected individuals;
- The maliciousness of the breach;
- Whether there are indications that personal information was misappropriated for nefarious purposes;
- The sensitivity of the information; and
- The harm that may result.

Significant harm means that it is important, meaningful and with non-trivial consequences or effects. For example, credit card fraud is described as a significant financial harm that can

be caused by a privacy breach. Credit card numbers with names are considered personal information of high sensitivity. There must also be a real risk of harm to individuals as a result of the breach. This does not require that harm will certainly result from the incident but that the likelihood that it will result must be more than a mere speculation. This standard was ruled to be satisfied when information such as financial information is accessed without authorisation and in a way that indicates nefarious purposes.

An organisation is responsible for personal information that is in its custody or under its control. Control is defined as having the authority to manage the personal information. An organisation engaging the services of a person, whether as an agent, by contract or otherwise, is responsible for that person's compliance with PIPA. If the data processor is outside of Canada, the entity will have to be in custody or control of personal information and have a real and substantial connection with Alberta for Alberta law to apply. There is a multi-factor test that exists for the purpose of determining whether a real and substantial connection exists, and there is at least one case that says that Canadian privacy law applies to a company in the U.S. that is collecting information on and providing information to Canadians.

Ontario

The following types of data must be breached to trigger notification:

- Information that identifies an individual; or
- Information for which it is reasonably foreseeable in the circumstances that it could be utilized, either alone or with other information, to identify an individual, in oral or recorded form, if the information:
  - i) relates to the physical or mental health of the individual, including information that consists of the health history of the individual's family;
  - ii) relates to the providing of health care to the individual, including the identification of a person as a provider of health care to the individual;
  - iii) is a plan of service developed by an approved agency for the individual;
  - iv) relates to payments or eligibility for health care, or eligibility for coverage for health care, in respect of the individual;
  - v) relates to the donation by the individual of any body part or bodily substance of the individual or is derived from the testing or examination of any such body part or bodily substance;
  - vi) is the individual's health number; or
  - vii) identifies an individual's substitute decision-maker.

- Individuals must be notified if this information is stolen, lost or accessed by unauthorized persons.

The obligation to notify generally applies to:

i) health information custodians;

ii) people that health information custodians disclosed personal health information to; or

iii) people who collect or use health numbers, or who have had health numbers disclosed to them.

Newfoundland and Labrador

Where a custodian reasonably believes that there has been a material breach involving the unauthorised collection, use or disclosure of personal health information, the custodian shall inform the privacy commissioner of the breach. ("Custodians" are certain classes of people described in the relevant legislation who have custody or control of personal health information as a result of or in connection with the performance of the person's powers or duties.) Also, a custodian of personal health information shall notify the affected individual where the information is stolen, lost, disposed of in an unauthorized manner, or disclosed or accessed by an unauthorised person, unless the custodian doesn't believe that the breach will have an adverse impact upon the provision of health care or benefits to the individual, or on the well-being of the individual.

New Brunswick

A custodian shall notify the individual to whom the information relates and the provincial privacy commissioner at the first reasonable opportunity if personal health information is:

i) stolen,

ii) lost,

iii) disposed of except as permitted by relevant legislation,

iv) disclosed to or accessed by an unauthorized person,

unless the custodian reasonably believes that the breach will not have an adverse effect on the provision of health care or benefits to the individual, have an adverse effect on the well-being of the individual, or lead to the identification of the individual to whom the information relates.

Custodians in the province of New Brunswick are individuals or organisations that collect, maintain or use personal health information for the purpose of providing or assisting in the provision of health care or treatment or the planning and management of the health care system or delivering a government program or service.

Nova Scotia

As of June 1, 2013, a custodian taking the same meaning as in Newfoundland and Labrador, shall notify an individual if the health professional reasonably believes that:

i) their information is stolen, lost or subject to unauthorized access, use, disclosure, copying or modification; and

ii) as a result, there is potential for harm or embarrassment to the individual.

Where a custodian makes the decision not to notify an individual, the custodian shall notify the provincial privacy review officer as soon as possible.

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?

Alberta

Notifications to the Alberta Commissioner must include a description of:

- The circumstances of the breach;
- The date on which or time period during which the breach occurred;
- The personal information involved in the breach;
- The risk of harm to individuals as a result of the breach;
- The number of individuals to whom there is a real risk of significant harm as a result of the breach;
- Any steps the organisation has taken to reduce the risk of harm;
- Any steps the organisation has taken to notify individuals; and
- Contact information for a person who can answer, on behalf of the organisation, questions about the breach.

There is also a specific form that organisations may use when reporting a security breach.

Notifications to individuals must include a description of:

- The circumstances of the breach;
- The personal information involved;
- Any steps the organisation has taken to reduce the risk of harm;
- The date on which or time period during which the breach occurred;
- Contact information for a person who can answer, on behalf of the organisation, questions about the breach.

The notice must be given without unreasonable delay. If the Alberta Commissioner requires the organisation to notify an individual, the Alberta Commissioner may determine the time period within which this must be done and reflect this in the Commissioner's notification decision.

Notifications that must be made to the Alberta Commissioner must be in writing. Notification to individuals must be given directly to the individual, unless the Alberta Commissioner determines that direct notification would be unreasonable—then indirect notification is acceptable.

Ontario

The notice must be given at the first reasonable opportunity (subject to certain exceptions).

There is no method of notification specified or any required or suggested content.

Newfoundland and Labrador

The notice must be given to the affected individual at the first reasonable opportunity (subject to certain exceptions).

There is no method of notification specified.

New Brunswick

The notice must be given at the first reasonable opportunity but there is no method of notification specified.

Nova Scotia

The notice must be given at the first reasonable opportunity but here is no method of notification specified.

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

Alberta

PIPA provides for a fine of no more than $100,000 for organisations and $10,000 for individuals who fail to notify the Alberta Privacy Commissioner when required to. As a practical matter, the main risks are adverse publicity or a binding order being made to do or not do an activity.

Ontario

Wilful disclosure of personal health information in contravention of relevant legislation is an offence, as is wilfully obstructing the Ontario Privacy Commissioner in the performance of his

or her functions. These offences, amongst others, are punishable by a fine of no more than $250,000. As a practical matter, the main risks are adverse publicity or a binding order being made to do or not do an activity.

Newfoundland and Labrador

Wilful disclosure or use of personal health information in contravention of relevant legislation is an offence, as is wilfully obstructing the Newfoundland and Labrador Privacy Commissioner in the performance of his or her functions. These offences, amongst others, are punishable by a fine of not more than $10,000 or to imprisonment for a term not exceeding 6 months, or both. As a practical matter, the main risks are adverse publicity or a binding order being made to do or not do an activity.

New Brunswick

Wilful disclosure or use of personal health information in contravention of relevant legislation is an offence, as is wilfully obstructing the New Brunswick Privacy Commissioner in the performance of his or her functions. These offences, amongst others, are punishable by a fine of between $240 and $10,200 for a first offence. As a practical matter, the main risks are adverse publicity or a binding order being made to do or not do an activity.

Nova Scotia

Wilful disclosure of personal health information in contravention of relevant legislation is an offence, as is wilfully obstructing or making a false statement to the provincial review officer. These offences, amongst others, are punishable, in the case of a corporation, by a fine of not more than $50,000. As a practical matter, the main risks are adverse publicity or a binding order being made to do or not do an activity.

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)?

This question is answered only for the federal private sector privacy law and the Provinces of Ontario (non-health) and Quebec.

All of the usual factors should be taken into account in deciding whether to notify, including the risk of harm, level of expected harm to individuals, and what the individuals can do to protect themselves in light of the breach.

Generally, where the breach creates a risk of harm to individuals, notification is encouraged as this will allow individuals to take steps to minimise harm.

The Office of the Privacy Commissioner of Canada has issued a set of best practices guidelines (the "Guidelines") that organisations are actively encouraged to follow when responding to privacy breaches.

With respect to notification requirements, and specifically when notification should be given, the Guidelines provide that the key consideration in deciding whether to notify affected individuals should be whether notification is necessary in order to avoid or mitigate harm to an individual whose personal information has been inappropriately accessed, collected, used or disclosed. Therefore, if a breach creates a risk of harm to the individual, those affected should be notified in order to help such individuals mitigate the damage by taking steps to protect themselves. Each incident needs to be considered on a case-by-case basis to determine whether privacy breach notification is required.

The Guidelines provide for a series of questions organisations need to consider when assessing whether the privacy breach creates a risk of harm to the individual and whether the individual should be notified. These are:

- What is the risk of harm to the individual? Specifically:
  - Is there a reasonable risk of identity theft or fraud (usually because of the type of information lost, such as an individual's name and address together with government-issued identification numbers or date of birth);
  - Is there a risk of financial harm to the individual (usually a loss of money or other assets, income, business opportunity or employment);
  - Is there a risk of physical harm (does the loss put an individual at risk of physical harm, stalking or harassment); or
  - Is there a risk of humiliation or damage to the individual's reputation (e.g., when the information lost includes mental health, medical or disciplinary records)?
- What is the ability of the individual to avoid or mitigate possible harm if he or she is informed?
- What are the reasonable expectations of the individual concerned (would the individual reasonably expect to be notified of the breach under the circumstances)?
- What are the legal and contractual obligations of the organisation towards the individual (does the organisation have a contractual obligation to inform the individual of the breach)?
- How sensitive is the information (generally, the more sensitive the information, the higher the risk of harm to individuals)?

It should be noted that certain types of personal information have been determined to be more sensitive than others. For example, health information, government-issued pieces of identification such as social insurance numbers, driver's license and health care numbers, and financial account numbers such as credit or debit card numbers that could be used in combination for identity theft, are the most sensitive types of personal information. However, sensitivity alone is not the only criteria in assessing the risk, as foreseeable harm to the individual is also important.

A complete pdf version of the Guidelines and summary checklist is available at:

- www.priv.gc.ca/information/guide/2007/gl_070801_02_e.pdf;
- www.priv.gc.ca/information/guide/2007/gl_070801_checklist_e.pdf.

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

- Alberta: Personal Information Protection Act, S.A. 2003, c. P-6.5.
- Ontario: Personal Health Information Protection Act, S.O. 2004, c. 3, Sch. A.
- Newfoundland and Labrador: Personal Health Information Act, S.N.L. 2008, c. P-7.01.
- New Brunswick: Personal Health Information Privacy and Access Act, S.N.B. 2009, c. P-7.05.
- Nova Scotia: Personal Health Information Act, S.N.S. 2010, c. 41.

7. Contact information for Data Protection Authority:

Federal

Name:	Office of the Privacy Commissioner of Canada
Address:	112 Kent Street, Place de Ville, Tower B, 3rd Floor, Ottawa, Ontario K1A 1H3
Telephone:	+1 613 995 2042 or +1 800 282 1376
Fax:	+1 613 947 6850
Email:	notification@priv.gc.ca
Website:	www.priv.gc.ca

Alberta

Name:	Office of the Information and Privacy Commissioner (Calgary)
Address:	Suite 2460, 801 6 Avenue SW, Calgary AB, T2P 3W2
Telephone:	+1 403 297 2728 or +1 888 878 4044
Fax:	+1 780 422 5682
Email:	generalinfo@oipc.ab.ca
Website:	www.oipc.ab.ca

Ontario

Name:	Information and Privacy Commissioner/Ontario
Address:	2 Bloor Street East, Suite 1400, Toronto, Ontario M4W 1A8
Telephone:	+1 416 326 3333
Fax:	+1 416 325 9195
Email:	info@ipc.on.ca
Website:	www.ipc.on.ca

Newfoundland and Labrador

Name:	Office of the Information and Privacy Commissioner Newfoundland and Labrador
Address:	2nd Floor, 34 Pippy Place, P.O. Box 13004, Station A, St. John's, NL, A1B 3V8
Telephone:	+1 709 729 6309
Fax:	+1 709 729 6500
Email:	commissioner@oipc.nl.ca
Website:	www.oipc.nl.ca

New Brunswick

Name:	Access to Information and Privacy Commissioner's Office
Address:	65 Regent Street, Suite 230, Fredericton, NB E3B 7H8
Telephone:	+1 506 453 5965
Fax:	+1 506 453 5963
E-mail:	access.info.privacy@gnb.ca
Website:	www.info-priv-nb.ca

Nova Scotia

Name:	The Nova Scotia Freedom of Information and Protection of Privacy Review Office
Address:	Box 181, Halifax, NS, B3J 2M4
Telephone:	+1 902 424 4684
Fax:	+1 902 424 8303
Email:	Not available
Website:	www.foipop.ns.ca

For more information, contact:

Name:	Lauren MacLeod
Firm:	Goodmans LLP
Address:	Bay Adelaide Centre, 333 Bay Street, Suite 3400 Toronto, Ontario, M5H 2S7 Canada
Telephone:	+1 416 597 6267
Fax:	+1 416 979 1234
Email:	lmacleod@goodmans.ca
Website:	www.goodmans.ca

Name:	George J. Pollack
Firm:	Davies Ward Phillips & Vineberg
Address:	1501, av. McGill College, suite 2600, Montréal (Québec) Canada H3A 3N9
Telephone:	+1 514 841 6420
Fax:	+1 514 841 6499
Email:	gpollack@dwpv.com
Website:	www.dwpv.com

CHILE

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)?**

   No. There is no legal obligation or requirement under Chilean law to notify the affected individuals and/or any authority in case of a data breach. In Chile there is no data protection authority, and each affected person must enforce the law individually through the Ordinary Courts of Justice.

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?**

   Not applicable.

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?**

   Not applicable.

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

   Not applicable.

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)?**

   Even though there is no legal obligation, it may be advisable to consider a notification to individuals in order to reduce potential damages and exposure under civil law.

   Although there are no specific fines or sanctions involved with data protection law breaches, any person responsible for a personal data database must indemnify economic and/or moral damages in case of improper treatment, without prejudice of having to eliminate, modify or block the corresponding data, upon request of the owner, or if ordered by court.

6. **What are the applicable data protection laws or guidelines within your country?**

   The relevant data protection law in Chile is Law No. 19,628 ("Personal Data Act") and recent Law No. 20,575. This Act establishes as a general principle that personal data can only be used when authorised by law or when the owner of the data gives a written and informed

consent. The data subject may revoke, at any time, his/her authorisation through a written communication directed to the entity that is currently processing the relevant data.

Sensitive Data is defined by the Personal Data Act as personal data which deals with the moral or physical characteristics of a person or to events or facts of his or her private life including religion, race, political views, sex life and health status. Sensitive information may only be transferred or used if authorisation is granted by law or by the owner of the data, or if such data is necessary for granting health benefits to such owner.

There are some exceptions to the obligation to obtain authorizations which are detailed below; however, in general terms the rights of the data subject may not be limited by any act or convention.

A private legal entity may handle personal data of its associates and of the entities to which they are affiliated without authorization, provided it is for the exclusive use of the entity and as far as it is used for statistic or rate-setting purposes, or for any general benefit of its associates or affiliate entities.

The Labour Code provides a general rule requiring employers to treat confidentially any private information and data in relation to their employees to which they have access as a result of the employment relationship.

No authorization from the owner of personal data is required in specific cases, such as the handling of personal data that comes or is collected from public sources that has a financial, bank or commercial nature, and this can only be disclosed when such information appears in commercial instruments, such as a protested bill.

Law No. 20.575 recently strengthened the protection and treatment of personal, economic, financial, commercial, and banking data. As a consequence, companies are restricted in how they can reveal personal data to third parties, with the exception of disclosures for commercial and credit risk evaluation purposes. Also, companies are not allowed to request from individuals any personal data of a financial, banking or commercial nature for purposes of recruitment, emergency medical attention, or in order to apply to a public or governmental job.

7. Contact information for Data Protection Authority:

Not applicable.

For more information, contact:

Name:	Sergio Orrego Flory or Francisco della Maggiora Martínez
Firm:	Urenda Rencoret Orrego y Dorr
Address:	Avenida Andres Bello No 2711, Piso 16, Las Condes, Santiago de Chile, Santiago, Chile, 7550611
Telephone:	+56 2 499 5500 or +56 2 499 5500/5545
Fax:	+56 2 499 5555
Email:	sorrego@urod.cl or fdellamaggiora@urod.cl
Website:	www.urod.cl

CHINA

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)?

There is no general data protection law in China to notify data breaches to the affected individuals or to the regulator. However, there is a national standard of data protection, namely the "Information Security Technology Guideline for Personal Information Protection within Information Systems for Public and Commercial Services" (GB/Z 28828-2012, or the "Guideline"), which became effective on February 1, 2013. This is only a technical guidance and has no compulsory legal effect.

According to the Guideline, in the case where the personal information is leaked, lost or distorted, the "administrator of the personal information" shall promptly take relevant measures to prevent the aggravation of the damages and shall promptly notify the affected individual; in the case of a material event, the administrator shall promptly report to the administration of personal information protection. The "administrator of personal information" refers to any organization or institution that determines the purpose and method of personal information processing, actually controls personal information and processes personal information through information systems.

Although there is no general data protection law, several laws and regulations in specific industrial sectors illustrate the obligation to notify data breaches.

For example, in the telecommunication and internet services industry, pursuant to the Telecommunications Regulation of the PRC ("the Regulation"), effective on September 25, 2000, and the "Decision of the Standing Committee of the National People's Congress on Strengthening Internet Information Protection" ("the Decision"), effective on December 28, 2012, the telecommunication operator and the internet information service provider shall report certain data breaches to the competent telecommunication administration.

For another example, in the banking and finance industry, pursuant to the "Circular of the People's Bank of China on Personal Financial Information Protection by Banking Financial Institutions" ("the Circular") effective on May 1, 2011, the banking financial institution ("BFI") shall notify and report to the local branch of the central bank of China (the People's Bank of China or "the PBC") in case of certain data breaches.

The answers to the following questions will take the above two industries as examples.

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?

Under the Guideline, as mentioned in the response to Question 1, the data administrator has the obligation to notify in case personal information is leaked, lost or distorted. The personal information under the Guideline refers to any computer data that is capable of being processed by an information system, is related to a specific natural person and is capable of identifying such specific natural person alone or in conjunction with other information, including personal sensitive information and personal general information.

In the telecommunication and internet services industry, where the telecommunication operator discovers any illegal information being transmitted in the telecommunication network or the internet service provider discovers that any information published by its users is forbidden to be published or transmitted by laws and regulations, the operator shall immediately cease transmitting such information, preserve relevant records, and report the same to the competent telecommunication administration.

In the banking and finance industry, according to the Circular, where divulgence of personal financial information occurs to a BFI, or any BFI at a higher level discovers that any BFI at a lower level provides personal financial information to others in violation of regulations or commits other acts in violation of the Circular, such BFI is obliged to notify the local branch of the PBC. After receiving the report of the BFI, such branch of the PBC shall deal with the matter according to the circumstances and report to the PBC in a timely manner. The personal financial information mentioned herein refers to the personal information obtained, processed or stored by the BFI in business operation or through its access to the credit reporting system, the payment system or any other systems of the PBC, including personal identity information, personal property information, personal account information, personal credit information, personal financial transaction information, derivative information and other personal information obtained or stored in the process of establishing business relationships with individuals.

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?

Under the Guideline, the data administrator shall promptly notify the affected individuals or the administration of personal information protection. However, the Guideline doesn't provide any requirements regarding the content of the notice, the specific time period or the method of giving notice.

In the telecommunication and internet services industry, the Decision doesn't prescribe any requirements regarding the content of the notice, the time period and the method of giving notice.

In the banking and finance industry, according to the Circular, the BFI shall give notice on the date when the divulgence occurs or seven business days after a violation by the BFI at a lower level is discovered; the content of the notice shall include relevant information of the data breach as well as a preliminary disposal opinion.

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

In relation to a general breach, there is no general obligation to notify and therefore no penalties. As for specific industries, there are also no explicit penalties, fines or risks in failing to notify the data breaches. However, some general penalties, fines or risks may apply when the data breaches have caused material damages or losses.

In the telecommunication and internet services industry, in case of any act in violation of the Decision, such punishments as giving a warning or fine, confiscating illegal gains, revoking licenses or cancelling filing, closing websites, and forbidding relevant responsible persons to engage in the internet service business shall be imposed legally, which shall be recorded in the social credit archive and be published. Where such an act violates the security administration regulations, a penalty for administration of public security shall be imposed. In a case in which such an act constitutes a crime, criminal liability shall be investigated. In a case of infringement upon the civil rights and interests of others, civil liability shall be borne legally.

In the banking and finance industry, where the BFI is in violation of the provisions under the Circular, the PBC and its competent branches may take the following measures to deal with the matter:

a. Talking with the senior management personnel of the BFI, requiring such personnel to explain the situation;
b. Ordering the BFI to make corrections within a stipulated time limit;
c. Circulating a notice within the financial system;
d. Advising the BFI to punish senior management personnel directly in charge and other directly responsible personnel; and
e. Where a crime is suspected, transferring the matter to judicial organs for disposal according to law.

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)?**

Yes. Although there is no exact provision requiring a notification to individuals in the event of a data breach affecting residents in China, some general or specific laws or regulations have

incorporated that the measures shall be taken to prevent the increase of damages or losses in certain events.

For example, pursuant to the Decision, in the case that the personal electronic information collected by internet service providers or other entities is leaked, damaged or lost, the internet service providers or other entities shall promptly take remedial measures.

Normally, a notification to individuals in the event of data breach affecting residents will be a necessary remedial measure to mitigate the damage and will be recommended.

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

As mentioned in the response to Question 1, no comprehensive and general data protection law is currently applicable in China, and the Guideline is only a technical guidance with no compulsory legal effect.

Although there is no general data protection law, a number of general laws have incorporated certain provisions of personal privacy protection to illustrate the principle of data protection, including but not limited to:

- The PRC Constitution;
- The General Principles of the Civil Law of the PRC;
- The Tort Liability Law of the PRC; and
- The PRC Criminal Law and its Amendment VII.

In addition, some laws, regulations or circulars regarding specific industrial sectors also contain provisions on personal information/data protection, such as the Regulation, Decision and Circular mentioned above as well as some other regulations, including but not limited to:

- The Regulations on Credit Reporting Industry effective on March 15, 2013;
- The Interim Measures on Management of Personal Credit Information Basic Database effective on October 1, 2005;
- Measures for the Supervision and Administration of Credit Card Business of Commercial Banks effective on January 13, 2011;
- The Statistics Law of the PRC effective on January 1, 2010;
- The Resident Identity Cards Law of the PRC effective on January 1, 2004;
- The Social Insurance Law of the PRC effective on July 1, 2011; and
- The Passport Law of the PRC effective January 1, 2007.

7. Contact information for Data Protection Authority:

In the PRC, the entity that is the relevant data protection authority will vary depending on the data protection area involved.

Mainly, the Ministry of Industry and Information Technology of the People's Republic of China ("MIIT") is the regulatory authority for data protection. Different departments under the internal hierarchy of MIIT also have different governing scope, for example: the Department of Policy and Law is in charge of drafting and amending the relevant laws and regulations regarding data protection and the Telecommunication Management Bureau is in charge of regulation of the telecommunication industry.

Other than MIIT, the State Internet Information Office will be in charge in the case of internet management; the Public Security Bureau will be in charge in the criminal case regarding data violation and breach.

For the sake of simplicity, below we provide only the contact information for MIIT:

Name:	Ministry of Industry and Information Technology of the People's Republic of China
Address:	No. 13, Changan Avenue West, Beijing, P.R. China
Telephone:	+86 10 6820 8025 (Administrative Office)
Website:	www.miit.gov.cn/n11293472/index.html

For more information, contact:

Name:	Jianwen Huang
Firm:	King & Wood Mallesons
Address:	40th Floor, Office Tower A, Beijing Fortune Plaza, 7 Dongsanhuan Zhonglu, Chaoyang District, Beijing 100020, P. R. China
Telephone:	+86 10 5878 5165
Fax:	+86 10 5878 5599
Email:	huangjianwen@cn.kwm.com
Website:	www.kwm.com

COLOMBIA

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)?**

   Currently, there is no legal obligation to notify the affected individual when there is a data breach. However, this obligation may be included in further regulation expected to be enacted by the Government in the months to come.

   In accordance with article 17 (n) and article 18 (k) of Statutory Law 1581 (2012), both the data controller and the data processor must inform the Superintendence of Industry and Trade ("DPA"), whenever a data breach is detected or when the management of the data is in danger.

   Pursuant to article 3 of Law 1581 of 2012, the parties involved in the treatment of data in Colombia are defined as: i) the data controller which is a private or public natural person or legal entity who, either individually or in association with third parties, controls the databases and the processing of said data, and ii) the data processor, which is a private or public natural person or legal entity who, either individually or in association with third parties, processes the data on behalf of the data controller.

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?**

   There are no specific requirements however there is an obligation to notify the DPA on breach of any information that can be associated with or linked to one or more identified or identifiable natural persons and notification should come from both the data controller and the data processor.

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?**

   There are no specific conditions that must be complied with in order to notify the DPA.

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

   For failing to comply with the obligations imposed under Statutory Law 1581 (2012), including the requirement to notify the DPA of a data breach, article 23 determines that the DPA can impose the following fines and penalties on the data controller and the data processor:

   a) Fines up to USD 2 million;

b) Suspension of the activities related to data collection, for up to 6 months;

c) Temporary closure of operations related to data collection and data treatment; and/or

d) Immediate and definitive closing of any operation that involves the processing of sensitive data.

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)?

There are no official recommendations regarding the need or recommendation to notify individuals in the event of a data breach.

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

The main data protection national laws and regulations are the following:

- Article 15 of the National Constitution, which defines the protection of Personal data as a fundamental right known as "*Habeas Data*";
- Statutory Law 1266 (2008), which sets out the legislation on personal databases, especially those related to financial, credit and commercial data, and services from other countries;
- Statutory Law 1581 (2012), which sets out the legislation on personal data protection; and
- Statutory Law 1273 (2009), which modified the Criminal Code and legislated to make the illegitimate acquisition, promotion, exchange or other misuse of personal data a crime.

7. Contact information for Data Protection Authority:

Note: As a general rule the Superintendence of Industry and Trade is the data protection authority in Colombia. The Superintendence of Finance (SFC) only has jurisdiction where the source of the information, the user of the information or the data operator is an entity monitored by the SFC (i.e. financial institutions).

Superintendence of Industry and Trade:

Name:	José Alejandro Bermúdez Durana (Deputy Superintendent for Personal Data Protection) or Carlos Enrique Salazar Muñoz (Director of the Personal Data Research Group) at the Superintendence of Industry and Trade - Personal Data Protection office
Address:	Bogotá, D.C., Colombia, Carrera 13, 27-00
Telephone:	+571 5870 247/227
Fax:	+571 5870 284
E-mail:	habeasdata@sic.gov.co or habeasdata@sic.gov.co

Superintendence of Finance:

Name:	Gerardo Hernández Correa (Superintendent of Finance)
Address:	Calle 7 No. 4-49
Telephone:	+571 594 0200/594 0201
Fax:	+571 350 7999/350 5707
E-mail:	ghernandez@superfinanciera.gov.co

For more information, contact:

Name:	Diego Cardona
Firm:	Prietocarrizosa
Address:	Carrera 9 # 74-08 of 305, Bogotá D.C., Colombia,
Telephone:	+571 326 8600 Ext. 1602
Fax:	+571 326 8610
Email:	dcardona@prietocarrizosa.com
Website:	www.prietocarrizosa.com

CZECH REPUBLIC

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)?**

   Specific data breach procedures are required only in the area of electronic communications. Providers must notify:

   - The DPA without delay, including a description of the effects of the breach with measures taken or proposed in reaction;
   - The individual concerned and the DPA if the breach is of such nature that it may seriously infringe on the privacy of an individual, or if the electronic services provider has not taken remedial measures in line with the DPA's assessment;
   - The individual concerned, if the DPA, after an investigation of the breach, orders the service provider to do so and if it has not done so already.

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?**

   Notification must be given in accordance with question 1 above where there is a breach of any personal data. The entity is defined solely as "provider of publicly accessible telecommunications services". This narrows the scope of obliged entities as the general data protection legislation (the Act on the Protection of Personal Data) does not require data breach notification. It follows that the electronic services provider can be either data controller or processor.

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?**

   The notice must generally include information on the effects of the breach and technical security measures that have been taken or are being proposed. The notice must be given without undue delay and specific forms are published by the DPA at its web pages.

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

   The maximum penalty is up to CZK 20 million (approximately USD one million).

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)?

Currently, notifying affected individuals of data breaches in areas other than electronic communications is not usual practice. However, this is advisable because of the general statutory obligation to limit damage, especially in cases where potential damages could be high.

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

The main data protection national laws and regulations are:

- Act No 101/2000 Coll., on Protection of Personal Data; and
- Act No 127/2005 Coll., on Electronic Communications.

7. Contact information for Data Protection Authority:

Name:	Úřad pro ochranu osobních údajů Pplk
Address:	Sochora 27, 170 00 Praha 7, Prague, Czech Republic
Telephone:	(Information) +420 234 665 555 or (Switchboard) +420 234 665 111
Fax:	+420 234 665 444
Email:	posta@uoou.cz
Website:	www.uoou.cz

For more information, contact:

Name:	Petr Kadlec or Richard Otevřel
Firm:	Havel, Holásek & Partners
Address:	Týn 1049/3, Prague, 110 00, Czech Republic
Telephone:	+420 224 895 844 or +420 224 895 943
Fax:	+420 224 895 980
Email:	petr.kadlec@havelholasek.cz or richard.otevrel@havelholasek.cz
Website:	www.havelholasek.cz

DENMARK

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)?**

   No, there is no requirement to notify either individuals or a regulator.

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?**

   Not applicable.

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?**

   Not applicable.

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

   Not applicable.

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)?**

   Yes, the Danish Data Protection Agency recommends that individuals are to be notified in case of data breach. The Danish Data Protection Agency may also request that the data controller provides certain information relating to the data breach and the security measures taken in order to limit the damages and prevent future data breaches.

6. **What are the applicable data protection laws or guidelines within your country?**

   The key legislation is the Danish Act on Processing of Personal Data, cf. Act no. 429 of 31 May 2000. In addition the Danish Data Protection Agency has issued a number of guidelines regarding various data protection matters.

7. Contact information for Data Protection Authority:

Name:	Danish Data Protection Agency (*Datatilsynet*)
Address:	Borgergade 28, 5, 1300 København K., (Copenhagen, Denmark)
Telephone:	+45 33 19 32 00
Fax:	+45 33 19 32 18
Email:	dt@datatilsynet.dk
Website:	www.datatilsynet.dk

For more information, contact:

Name:	Marie Albæk Jacobsen or Charlotte Bagger Tranberg
Firm:	Bech-Bruun
Address:	Langelinie Allé 35, 2100 Copenhagen, Denmark
Telephone:	+45 72 27 3349 or +45 72 27 3476
Fax:	+45 72 27 0027
Email:	maja@bechbruun.com or cbt@bechbruun.com
Website:	www.bechbruun.com

FINLAND

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)?**

   If there is a specific violation, or risk of such a violation, of the security of information in relation to a telecommunications service, the telecommunications operator and service provider shall immediately notify the users and subscribers. The telecommunications operator only (not the service provider) must notify the Finnish Communications Regulatory Authority (FICORA) without undue delay of all significant information security violations and threats thereof.

   These obligations do not apply to a data controller in any other situation.

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?**

   There is no categorization of data types that would or would not trigger either of the notification obligations in Question 1 above. Furthermore, Finnish statutory legislation does not provide any further explanation about the characteristics of significant or specific violations.

   However, FICORA has issued a regulation (FICORA 9 D/2009 M) providing a list of examples, which could determine whether a violation is significant and/or specific. The obligations apply only to telecommunications operators and/or value-added service providers, not a data controller in any other situation.

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?**

   Finnish legislation does not set forth requirements concerning the content of the notice but FICORA has issued regulations on the content and form of the notifications.

   If there is a specific threat directed at a network or services, a notification has to be sent to the customers and/or subscribers either by email or putting a notice on the company's website.

   Also, FICORA has to be notified if there is a significant data security threat (such as a data breach, malware or social engineering) directed at the communication network. The company has to send a written notice to the authority. If the situation is urgent, an initial notification can be made via telephone, followed by a written notice.

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

   Anyone who deliberately neglects the notification requirement may be subject to a fine for a violation of protection of privacy in electronic communications.

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)?**

   There is no general obligation to notify data subjects about data breaches. However it is recommended that a data controller sends an informal notice to data subjects whose data has been endangered so that the data subject is alerted about possible misuse of his/her personal data.

6. **What are the applicable data protection laws or guidelines within your country?**

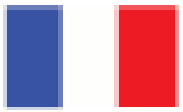
   Act number 516/2004 provides special regulation on confidentiality in electronic communications as well as the handing and processing of communications identification data and location data. The rules on data breach notification obligations detailed in the answers above are set forth in this Act.

7. **Contact information for Data Protection Authority:**

Name:	Tietosuojavaltuutetun toimisto
Address:	PL 315, 00181 Helsinki, Finland
Telephone:	+358 (0)10 36 66700
Fax:	+358 (0) 29 56 66735
Email:	tietosuoja@om.fi
Website:	www.tietosuoja.fi

For more information, contact:

Name:	Eija Warma or Otto Markkanen
Firm:	Castrén & Snellman Attorneys Ltd
Address:	PO Box 233 (Eteläesplanadi 14), FI-00131 Helsinki, Finland
Telephone:	+358 (0) 20 7765 765
Fax:	+358 (0) 20 7765 001
Email:	eija.warma@castren.fi or otto.markkanen@castren.fi
Website:	www.castren.fi



FRANCE

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, there is a legal obligation to notify a data breach to the French data protection authority ("CNIL") and the affected individuals but only under certain conditions related to public electronic communications services (see below).

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?**

   A data breach is defined as "any security breach that accidentally or unlawfully results in the destruction, loss, alteration, disclosure or unauthorized access to personal data that is being processed in connection with the provision of publicly available electronic communications services."

   Data controllers that are providers of public/publicly available electronic communication services (such as internet service providers and telecoms providers) must notify the CNIL of data breaches. All data breaches that affect publicly electronic communication services need to be reported, regardless of the severity.

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?**

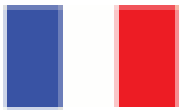
   The provider of publicly available electronic communications services must, without delay, notify the personal data breach to the CNIL.

   To notify a data breach, written notification must be sent to the CNIL, stating:

   - The nature and consequences of the breach;
   - The measures already implemented or proposed to remedy to the breach;
   - The names of the individuals who can provide additional information; and
   - If possible, an estimate of the number of individuals potentially affected by the breach.

   There is no legal requirement regarding the method of giving notice. It is recommended to use certified mail with a return receipt requested.

   The provider must notify individuals without delay only if the personal data breach is likely to adversely affect their personal data or privacy. If the provider decides not to notify affected individuals of the breach (i.e. presumes that there is no risk of damage to personal data or



privacy), it needs to inform the CNIL in its notification that appropriate measures of protection have been implemented to render the data unintelligible to any person who is not authorized to access it (e.g., technical measures such as encryption to prevent hackers from accessing data), and that those measures were applied to the data concerned by the security breach. To do so, the provider must provide the CNIL with:

- The name, address and phone number of the data controller;
- A full description of the measures of protection;
- The measures applied to guarantee their efficacy;
- If applicable, the reference number of the previous declaration/application to the CNIL related to the processing of personal data; and
- An explanation of whether it has notified or not individuals concerned and, if not, the reasons of the absence of notification.

The CNIL will make a decision on the need to notify the individuals within two months:

- If it considers that the implemented protective measures are appropriate, it will acknowledge their efficacy and confirm that it is not required to inform affected individuals;
- Otherwise, or if the CNIL does not reply within two months, the provider is required to notify individuals. In case of a severe data breach, the CNIL may send a legal notice to the service provider requiring it to notify individuals during the period it designated, a timeframe not exceeding one month.

Notification of a data breach to individuals can be achieved by any means, stating the following:

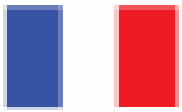
- The nature of the breach;
- The names of the individuals who can provide additional information about the breach;
- The measures recommended by the service provider to mitigate the consequences of the breach.

There is no legal requirement regarding the method of giving notice. It is however advisable to use certified mail.

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

Failing to notify when it is required to do so is an infringement of the French Data Protection Act, which entitles the CNIL to impose sanctions (warnings, injunctions, orders to stop processing operations, and financial sanctions up to €300,000). It is also a criminal offence, punishable by up to five years of imprisonment and a €300,000 fine.

In civil litigation, any person affected by the violation of personal data would be entitled to receive compensation for loss or damage.



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)?**

   The legal obligation to notify a data breach has a limited scope. In the event that the legal obligation to notify is not applicable, the CNIL advises notification of individuals so as to mitigate the consequences of the breach, since the data controller could still be held liable for the breach on the basis of the general data security obligations.

6. **What are the applicable data protection laws or guidelines within your country?**

   The key legislation is Act Number 78-17 of January 6, 1978 on Data Processing, Data Files and Individual Liberties.

7. **Contact information for Data Protection Authority:**

Name:	Commission Nationale de l'Informatique et des Libertés
Address:	8, rue Vivienne, CS 30223, 75083 Paris Cedex 02, France
Telephone:	+33 (0)1 53 73 22 22
Fax:	+33 (0)1 53 73 22 00
Email:	See website
Website:	www.cnil.fr

For more information, contact:

Name:	Laure Marolleau
Firm:	Soulier Avocats
Address:	2 Avenue Hoche, 75008 Paris, France
Telephone:	+33 (0)4 72 82 20 80
Fax:	+33 (0)4 72 82 20 90
Email:	l.marolleau@soulier-avocats.com
Website:	www.soulier-avocats.com

GERMANY

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, depending on the type of data and the severity of the breach, both the affected individual and the regulator have to be informed under Section 42a of the German Data Protection Act, (*Bundesdatenschutzgesetz*), ("BDSG").

   The notification obligation relates to controllers that are subject to the BDSG, irrespective of the location of the affected data subjects. The mere fact that a German resident's data is affected by a breach does not automatically trigger a notification obligation under the German provisions.

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?**

   The obligation will be triggered where a (private) controller determines that records of any of the following types of data have been unlawfully transferred or otherwise unlawfully disclosed to third parties, and as a result there is a threat of serious harm to the rights or legitimate interests of data subjects:

   - Special categories of personal data (i.e. information on racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, health or sex life);
   - Personal data subject to a professional secrecy (e.g. medical doctor's secrecy);
   - Personal data referring to criminal or administrative offences or to suspected criminal or administrative offences; or
   - Personal data concerning bank or credit card accounts.

   The obligation applies to data controllers only, therefore data controllers are under an obligation to take all necessary measures in order to comply with all breach notification obligations notwithstanding if a breach has been caused by the data controller him/herself or a data processor acting on his/her behalf.

   Data processors remain obligated to report any data breaches to the data controller in order to enable the data controller to fulfil his/her breach notification obligations in accordance with statutory requirements. It is therefore also required for data controllers and data processors to make provisions in any agreement between them for data breach notification stipulations (as required by Section 11 of the BDSG).

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?

The notification given to data subjects of any breach that concerns them must describe the nature of the unlawful disclosure and recommend measures to minimize possible harm. Neither legislation nor the relevant authorities provide any more detail on the requirements as to the extent of information to be provided regarding the nature of the unlawful disclosure. We would recommend that information on measures to minimise possible harm may include information on available technical security measures such as patches, other security software and/or updates, recommendations on change of passwords. Data subjects shall be informed as soon as appropriate measures to safeguard the data have been taken and notification would no longer endanger criminal prosecution.

The notification to the competent supervisory authority must be without delay and describe (in addition to the information provided to the data subjects) possible harmful consequences of the unlawful disclosure and measures taken by the body as a result.

For notifying data subjects and authorities there is no required form of notification (e.g. e-mail or written form). However, it would be advisable to conduct notification at least in textual form (e.g. e-mail) in order to allow for sufficient proof in case of legal disputes with concerned individuals and/or authorities. In general, data subjects must be notified individually. However, where notifying the data subjects would require a disproportionate effort, in particular due to the large number of persons affected, such notification may be replaced by public advertisements of at least one-half page in at least two national daily newspapers, or by another equally effective measure for notifying data subjects.

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

Violation of the notification obligations referenced above, by failing to notify or by doing so incorrectly, incompletely or outside the prescribed time limit, will be deemed an offence, whether committed intentionally or through negligence.

Such offence may be punished with a fine of up to €300,000 and the fine should exceed the financial benefit to the perpetrator derived from the offence. If €300,000 is not sufficient to do so, this figure may be increased.

In addition, anyone who wilfully commits such an offence in exchange for payment or with the intention of receiving a benefit, or of harming another person, shall be liable to imprisonment for up to two years or to a fine.

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)?

Not applicable.

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

The main data protection national laws and regulations are the following:

- Sections 42a, 43 (2) para. 7 and 44 German Federal Data Protection Act (*Bundesdatenschutzgesetz*, BDSG);
- Section 15a Telemedia Act (*Telemediengesetz*, TMG); and
- Sections 93 (3) and 109a (1) Telecommunication Act (*Telekommunikationsgesetz*, TKG).

7. Contact information for Data Protection Authority:

Offences have to be notified respectively with the competent state supervisory authorities for the non-public sector (*Aufsichtsbehörden der Länder*). The competent authority will have to be determined in the individual case based on the place of business of the respective company. An overview on the most recent contact details for all state authorities is currently available at: www.bfdi.bund.de/EN/AdressesAndLinks/AufsichtsbehoerdenNichtOeffentlich/AufsBehoerdFuerDenNichtOeffBereich_node.html

For more information, contact:

Name: Dr. Kai Westerwelle or Thomas Kahl
Firm: Taylor Wessing
Address: Senckenberganlage 20-22, 60325 Frankfurt am Main, Germany
Telephone: +49 (0)69 9 71 30 110
Fax: +49 (0)69 9 71 30 100
Email: k.westerwelle@taylorwessing.com or t.kahl@taylorwessing.com
Website: www.taylorwessing.com

Or

Name: Christian M. Runte
Firm: CMS Hasche Sigle
Address: Partnerschaft von Rechtsanwälten und Steuerberatern, Nymphenburger Straße 12, 80335 München, Germany
Telephone: +49 89 238 07 163
Fax: +49 89 238 07 40804
Email: christian.runte@cms-hs.com
Website: www.cms-hs.com

GREECE

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)?**

   No, under Law 2472 /1997 (which is the general law regarding the protection of personal data in Greece), in the event of a data breach, there is no legal obligation or requirement to notify either the affected individuals or the DPA.

   However, according to article 12, paragraph 5 of Law 3471/2006 (which is a specific law regarding the protection of personal data and privacy in the electronic communications sector), in the event of a personal data breach, the provider of a publicly available electronic communications service must notify the Authority for Communication Security and Privacy (ADAE) and DPA without undue delay. Furthermore, according to paragraph 6 of the same article, in case of a personal data breach that may have detrimental consequences to the data owner, the provider has to notify the affected person without undue delay. It is not necessary to notify the affected person however, if the provider has proved to the competent authorities in a satisfactory manner that it has applied the appropriate technical security measures and that these measures were applied to the data related to the security breach according to paragraph 7 of article 12.

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?**

   The provider, who in this case acts as a controller, should notify of the data breach regarding the electronic communication sector irrespective of the type of data breached.

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 case of a data breach regarding the electronic communications sector, the notification must include at least a description of the nature of the personal data breach and the contact points from which further information can be obtained from the provider to deal with the breach. This notification must be given without undue delay. Law 3471/2006 does not provide a method of giving notice.

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

   Pursuant to Law3115/2003 article 11, in case of breach of the present law in relation to the privacy in the telecommunications sector or the revocation of its terms and procedures, the

Hellenic Authority for Communication Security and Privacy ("ADAE") is empowered to impose the following sanctions on any natural person or legal entity:

- A warning with a definite deadline within which the violation should cease; or
- A fine amounting between €15,000 and €1,500,000.

These administrative sanctions shall only be imposed following the issuance of a substantiated decision of the ADAE and following a hearing of the interested parties.

Any natural person or legal entity, which in breach of this law causes material damage shall be liable for damages in full and in the case of non-pecuniary damage, they shall be liable for compensation. The compensation payable, according to article 932 of the Civil Code for non-pecuniary damage, is set at a minimum of €10,000, unless a lesser amount is claimed. Such compensation shall be awarded irrespective of the claim for damages.

The claims referred to in the present Article shall be litigated according to articles 664-676 of the Code of Civil Procedure, notwithstanding whether the Data Protection Authority has issued a relevant decision on the ascertainment of criminal activities or criminal charges.

Custodial sentences may be given in the following circumstances:

- Anyone who unlawfully interferes in any way whatsoever with a personal data file of a subscriber or user, or takes notice of such data or extracts, alters, affects in a harmful manner, destroys, processes, transfers, discloses, makes accessible to unauthorised persons or permits such persons to take notice of such data or anyone who exploits such data in any way whatsoever, will be punished by imprisonment for a period of at least one(1) year and a fine of between €10,000 and €100,000, unless otherwise subject to more serious sanctions;
- Any Controller or representative thereof who does not comply with the acts of the Data Protection Authority (imposing the administrative penalties of provisional licence revocation, file destruction or interruption of processing of the pertinent data), will be punished by imprisonment for a period of at least two years and a fine of between €12,000 and €120,000;
- If the perpetrator of the acts referred to above gained unlawful benefit on their own or on another person's behalf or intended to cause harm to a third party, then they shall be punished with imprisonment for a period of up to 10 years and a fine amounting €15,000 and €150,000;
- If this endangers the free operation of the democratic constitution or national security, the perpetrator shall be punished with imprisonment and a fine of between €50,000 and €350,000;
- If the perpetrator of the acts committed these by negligence, then they shall be punished with imprisonment for a period of up to 18 months and a maximum fine of €10,000.

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)?**

   Even though it is not provided by law it is advisable.

6. **What are the applicable data protection laws or guidelines within your country?**

   The main data protection national laws and regulations are Law 2472/1997 and Law 3471/2006.

7. **Contact information for Data Protection Authority:**

Name:	Hellenic Data Protection Authority Offices
Address:	Kifissias 1-3, 115 23 Athens, Greece
Telephone:	+30 210 647 5628
Fax:	+30 210 647 5600
Email:	Not Available
Website:	www.dpa.gr

For more information, contact:

Name:	Popi Papantoniou
Firm:	Bahas, Gramatidis & Partners
Address:	Filellinon Street 26, Athens 105 58, Greece
Telephone:	+30 120 331 8170
Fax:	+30 120 331 8171
Email:	p.papantoniou@bahagram.com
Website:	www.bahagram.com

HONG KONG

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)?**

   There is currently no legal obligation or requirement to notify the affected data subjects or the regulator (i.e. Office of the Privacy Commissioner for Personal Data or "PCPD") in the event of a data breach affecting residents in Hong Kong.

   However, note that the PCPD has issued a Guidance Note on Data Breach Handling and the Giving of Breach Notifications in June 2010 ("Guidance Note"). Although the Guidance Note confirms that notification of a data breach to the PCPD is not legally required under the Personal Data (Privacy) Ordinance (Cap 486 or "the Ordinance"), it is prudent and advisable for data users to maintain a system of notification in handling a data breach. In particular, in the event of a data breach, the data user should consider the circumstances of the case and determine whether any of the following persons should be notified as soon as practical:

   - The affected data subjects;
   - The PCPD;
   - The law enforcement agencies;
   - Any relevant regulators;
   - Such other parties who may be able to take remedial actions to protect the personal data privacy and the interests of the affected data subjects (for example, internet companies like Google and Yahoo may assist to remove the relevant cached link from its search engine).

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?**

   A data breach is generally taken to be a suspected breach of data security of personal data held by a data user, exposing this data to the risk of loss, unauthorised or accidental access, processing, erasure or use. Given there is no legal requirement to notify the PCPD of a data breach, the conditions under which such notification must be given and the types of data that must be breached to trigger notification may depend on the circumstances and the impact of the data breach. Where data subjects can be identified and real risk of harm is reasonably foreseeable, a data user should seriously consider notifying the data subjects, the PCPD and the relevant parties.

   Having assessed the situation and the impact of the data breach, the notification should be made by the data user as soon as practicable. A data user, in relation to personal data, means a person who, either alone or jointly or in common with other persons, controls the collection, holding, processing or use of the data.

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?

Depending on the circumstances of each case, the notification may include the following information:

- A general description of what occurred;
- The date and time of the breach and its duration, if applicable;
- The date and time the breach was discovered;
- The source of the breach (either the data user itself or the third party that processed the personal data on its behalf);
- A list of the type of personal data involved;
- An assessment of the risk of harm (such as identity theft or fraud) as a result of the breach;
- A description of the measures taken or that will be taken to prevent further loss, unauthorised access to or leakage of the personal data;
- The contact information of a department or an individual designated by the data users within the organisation for affected data subjects to obtain more information and assistance;
- Information and advice on what data subjects can do to protect themselves from the adverse effects of the breach and/or against identity theft or fraud; and
- Whether law enforcement agencies, the PCPD and such other parties have been notified.

The Guidance Note provides that a data user should exercise care and prudence in determining the extent of the information, including personal data, to be included in the notification so as not to compromise the investigative works concurrently undertaken. The Guidance Note also provides a Data Breach Notification Form which can be used for giving notification of a data breach to the PCPD.

The Guidance Note does not specify any time limit regarding when a data breach must be notified. However, it provides that notification should be made as soon as practicable after the detection of the data breach, except where law enforcement agencies have for investigative purpose made a request for a delay.

The Guidance Note provides that the notification can be made by telephone, in writing, via email or in person. When data subjects are not identifiable immediately or where public interest exists, public notification would be the more appropriate means of effective communication, such as through website or media. Data users should also consider whether the method of notification adopted might increase the risk of harm.

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

   The PCPD is not empowered to impose any penalties or fines on the data user for failing to notify a data breach. Nonetheless, a promptly made data breach notification may reduce the risk of potential litigation, enable the affected data subjects to take appropriate protective measures and allow the data user to regain the goodwill of its data subjects.

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)?**

   Yes. Although there is no legal obligation or requirement to notify the affected data subjects or the PCPD of a data breach in Hong Kong, it would be prudent and advisable that a data user take active remedial measures promptly to mitigate the loss and damage that may be caused to the data subjects. The Guidance Note sets out the following action plan recommended by the PCPD in handling a data breach:

   - Immediate gathering of essential information relating to the breach (e.g. when, where and how the data breach occurred, the cause of the breach, the kind and extent of the personal data affected)
   - Adopting appropriate measures to contain the breach (e.g. stopping the relevant system, changing passwords and access rights to the data, notifying the relevant law enforcement agencies)
   - Assessing the risk of harm (e.g. the types of potential damage and the extent of such damage)
   - Considering giving data breach notification (in particular where data subjects can be identified and real risk of harm is reasonably foreseeable)

6. **What are the applicable data protection laws or guidelines within your country?**

   The principal data protection law in Hong Kong is the Personal Data (Privacy) Ordinance (Cap 486), which was enacted in 1995 to protect the personal data privacy of individuals.

   The Ordinance covers any personal data i.e. recorded information relating directly or indirectly to a living individual (data subject); from which it is practical to ascertain the identity of the individual; and in a form in which access to or processing of the data is practicable. It applies

to any person (data user, including private sector, public sector and government department) who controls the collection, retention, processing or use of personal data. It sets out six data protection principles (DPPs) governing the proper collection, accuracy, retention, use, security, access and correction of personal data in both the public and private sectors:

- The purpose and manner of collection of personal data. Personal data must be collected for a purpose directly related to a function and activity of the data user (i.e. to individual or company that came into possession of personal data) and data subjects shall be informed of the purpose for which the data are collected and to be used;
- The accuracy and retention of personal data. All practicable steps must be taken to ensure the accuracy of personal data and such data must be deleted upon fulfilment of the purpose for which the data are used;
- The use of personal data. Unless the data subject has given prior consent, personal data must be used for the purpose for which they were originally collected or a directly related purpose;
- The security of personal data. All practicable steps must be taken to ensure that personal data are protected against unauthorized or accidental access, processing or erasure;
- Information regarding policies and practices in relation to personal data must be made generally available; and
- Access to personal data. Individuals have rights of access to and correction of their personal data.

The independent Office of the Privacy Commissioner for Personal Data (PCPD) was established in 1996 with the mandate to promote good data protection practices and to oversee data users' compliance with Ordinance. Since its establishment, PCPD has issued various guidance to data users on different areas to promote good data protection practices.

In June 2012, the Legislative Council passed the Personal Data (Privacy) (Amendment) Ordinance (the Amendment Ordinance). The Amendment Ordinance introduced a number of changes to the Ordinance to enhance the protection of personal data privacy of individuals. The most significant changes relate to the use, transfer and sale of personal data for direct marketing and powers of the PCPD. A number of other changes relating to offences, penalties for breaches of the Ordinance and exemptions from various provisions of the Ordinance, have also been introduced. Most of the changes had came into effect on October 1, 2012 while certain provisions relating to direct marketing came into effect on April 1, 2013 and the provisions relating to the legal assistance scheme will take effect on another subsequent date to be announced by the Government.

Investigations about suspected breaches of the Ordinance may be carried out by the PCPD, either in response to a complaint or at its own initiative. If the PCPD concludes that a contravention is likely to be repeated, an enforcement notice may be issued and penalty may be imposed.

Individuals may also claim compensation through civil proceedings for damage caused to them as a result of a contravention of the Ordinance.

7. Contact information for Data Protection Authority:

Name:	Office of the Privacy Commissioner for Personal Data
Address:	12/F, 248 Queen's Road East, Wanchai, Hong Kong
Telephone:	+852 2827 2827
Email:	enquiry@pcpd.org.hk
Website:	www.pcpd.org.hk

For more information, contact:

Name:	Patrick Peng
Firm:	Edwards Wildman Palmer
Address:	Suite 2703, 27/F The Center, 99 Queen's Road Central, Hong Kong
Telephone:	+852 3150 1936
Email:	ppeng@edwardswildman.com
Website:	www.edwardswildman.com

INDIA

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)?**

   No, there is no legal obligation to notify either affected individuals or a regulator about any data breach.

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?**

   Not applicable.

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?**

   Not applicable.

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

   Not applicable.

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)?**

   No, unless it is desirable to notify the individuals so they can take action to minimize the impact of the data breach.

6. **What are the applicable data protection laws or guidelines within your country?**

   The applicable rules regarding data protection in India are the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, (the "Rules") formed by the Central Government of India in exercise of its powers conferred by clause (ob) of sub-section (2) of section 87 read with section 43A of the Information Technology Act, 2000.

   As per the Rules every "body corporate" that "collects, receives, possess, stores, deals or handles" any information including sensitive personal data and information is required to

provide a privacy policy for handling or dealing with such information. The term 'sensitive personal data and information' has been comprehensively defined and includes information relating to financial information, passwords, biometric information and call data records.

The Rules impose wide ranging obligations on a body corporate regarding usage, collection and transfer of personal information and implementation of reasonable security practices.

7. Contact information for Data Protection Authority:

Not applicable.

For more information, contact:

Name:	Bomi Daruwala
Firm:	Vaish Associates Advocates
Address:	Flat No 7, 10, Hailey Road, Connaught Place, New Delhi, DL 110001, India
Telephone:	+91 11 4249 2525
Fax:	+91 22 4213 4102
Email:	bomi@vaishlaw.com
Website:	www.vaishlaw.com

IRELAND

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)?

Data breach notification requirements derive from two distinct sets of rules: (i) the Code, which applies to all data controllers and data processors; and (ii) the Regulations, which apply to certain entities in the telecommunications sector. The Code is not legally binding, though the Data Protection Commissioner may argue that it reflects the requirements implicit from the fair processing principle.

In relation to affected individuals, under the Code, the data controller must immediately consider whether to notify the affected data subjects in situations where personal data has been put at risk of unauthorised disclosure, loss, destruction or alteration. There is a legal obligation under the Regulations for a provider of an electronic communications service or network to notify affected individuals where a "personal data breach" is likely to "adversely affect the personal data or privacy of a subscriber or individual". A "personal data breach" means "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed in connection with the provision of a publicly available electronic communications service in the European Union".

Under both the Code and Regulations, notification of affected individuals is not required if technological protection measures of a high standard render the data unintelligible to any person not authorised to access it.

Under the Code, all incidents in which personal data has been put at risk should be reported to the Data Protection Commissioner, unless:

- The data subjects have already been informed;
- The loss affects no more than 100 data subjects; and
- The loss involves only non-sensitive, non-financial personal data.

The Regulations place an obligation on a provider of an electronic communications service or network to notify the Data Protection Commissioner where there is a personal data breach.

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?

Under the Regulations, it is stated that the "undertaking" (i.e. provider of an electronic communications service or network) shall notify the breach. See Question 1 for further detail in relation to when the obligation is triggered.

For both the Code and the Regulations, "Personal data" is the type of data that must be breached to trigger notification. This is defined as data relating to a living individual who is or can be identified either from the data or in conjunction with other information that is in, or is likely to come into, the possession of the data controller.

Under the Code the obligation is on the data controller to notify the affected subjects and the data processor must notify all incidents of loss of control of personal data to the relevant data controller as soon as the data processor becomes aware of the incident.

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?

The Code provides that the notification to the Data Protection Commissioner should outline the circumstances surrounding the incident, but must not contain the personal data. The DPC may request a detailed notification subsequently addressing certain specified matters. There is no detail in the Code in relation to what should be disclosed to the data subjects.

Under the Regulations, a notification, to both the affected individual and the Data Protection Commissioner, must at least contain:

- A description of the nature of the personal data breach;
- A description of the contact points where more information can be obtained;
- A recommendation on measures to mitigate the possible adverse effects of the personal data breach; and
- Where the notification is to the Data Commissioner, a description of the consequences of, and the measures proposed to be taken by the undertaking to address, the personal data breach.

Under the Code, notification by the data controller to the DPC must be made within two working days of becoming aware of the incident and notification by the data processor to the data controller must be made as soon as the data processor becomes aware of the incident. Under the Regulations, notice should be given "without undue delay". Notification may be given by email, telephone or fax.

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

   As the Code is voluntary, there are no direct penalties or fines in failing to notify. However, should the Code be promulgated as law, penalties may be introduced.

   Furthermore, the Irish Data Protection Commissioner is of the view that the Code represents a "fleshing out" of the general statutory requirements to keep data secure and to process it fairly. In cases of non-notification, the DPC may launch an investigation to consider whether these general obligations have been breached.

   Under the Regulations, an undertaking may be liable to a fine of between €4,000 and €250,000 (for a body corporate) or €50,000 (for a natural person).

   A court may also order that any data that appears to be connected with the commission of the offence be forfeited or destroyed and any relevant data be erased. The Regulations also state that where an undertaking has not notified the subscriber or individual of the personal data breach, the Data Protection Commissioner may, having considered the likely adverse effects of the breach, require the undertaking to do so by serving an enforcement notice.

   A failure to notify may have negative public reputation consequences which should be considered also.

   If a data controller is aware of a data breach, and its failure to notify a data subject of the breach has adverse consequences for the data subject, it is conceivable that a data controller may be liable in damages for the damage suffered as a result for breach of a duty of care owed to the data subject.

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)?**

   This would depend on the nature of the breach including the type and volume of data involved, whether it is encrypted, whether the breach was a result of a deliberate act and the type of data subjects.

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

The main data protection national laws and regulations are the following:

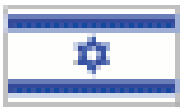
- Personal Data Security Breach Code of Practice (the "Code");
- European Communities (Electronic Communications Networks and Services);
- (Privacy and Electronic Communications) Regulations 2011 (the "Regulations"); and
- Data Protection Acts 1988 and 2003.

7. Contact information for Data Protection Authority:

Name:	Office of the Data Protection Commissioner
Address:	Canal House, Station Road, Portarlington, Co. Laois, Ireland
Telephone:	+353 (0)1 57 868 4800
Fax:	+353 (0)1 57 868 4757
Email:	info@dataprotection.ie
Website:	www.dataprotection.ie

For more information, contact:

Name:	Robert McDonagh
Firm:	Mason Hayes & Curran
Address:	South Bank House, Barrow Street, Dublin 4, Ireland
Telephone:	+353 1 614 5000
Fax:	+353 1 614 5001
Email:	rmcdonagh@mhc.ie
Website:	www.mhc.ie



ISRAEL

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)?**

   There is no statutory/regulatory requirement under Israeli law to notify the affected individuals or the DPA of a data breach affecting an Israeli resident.

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?**

   Not applicable.

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?**

   Not applicable.

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

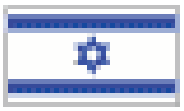
   Not applicable.

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)?**

   Notification of the affected individuals should be considered despite there being no obligation to do so, as this may help reduce possible damages and exposure under tort and contract law, if in the circumstances such damages are applicable.

6. **What are the applicable data protection laws or guidelines within your country?**

   The main data protection national law is the Protection of Privacy Law, 1981.



7. Contact information for Data Protection Authority:

Name:	The Israeli Law, Information and Technology Authority
Address:	The Government Campus, 9th floor, 125 Begin Road, Tel Aviv, Israel P.O. Box 7360, Tel Aviv 61072, Israel
Telephone:	+972 3 763 4050
Fax:	None available
Email:	ILITA@justice.gov.il
Website:	www.justice.gov.il/MOJEng/RashutTech/default.htm

For more information, contact:

Name:	Nurit Dagan Herzog, Fox and Neeman Law Office
Address:	Asia House, 4 Weizmann St, Tel Aviv 64239, Israel
Telephone:	+972 3 692 7424
Fax:	+972 3 696 6464
Email:	dagan@hfn.co.il
Website:	www.hfn.co.il

ITALY

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

   i) banks and financial institutions, and

   ii) public electronic communications providers.

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?**

   In relation to the obligation of notification by banks and financial institutions, for any data breach involving a bank's customer's data; in relation to the notification imposed on public electronic communication providers, for any breach of personal data involved in the providing of the communication services. The notification obligation is only on the controller.

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 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 and must be given without undue delays.

   Recently, the Italian DPA has issued a public consultation on data breach notification in the electronic communication field, proposing the time limits of 24 hours for a first brief notice and three days for a further detailed notice and recommending the publication and the web-posting of the notice.

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.

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)?**

   Provided that a case-by-case analysis is appropriate, in general terms, the notification is recommended even when it is not mandatory.

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 May 12th 2011; and
   - "Guidelines in the matter of implementation of the provisions on data breach notifications – Public consultation" of July 26, 2012.

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@garanteprivacy.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

JAPAN

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)?**

   No, there is no requirement in statute to notify either individuals or the data protection authority. However, Article 20 of the Act on the Protection of Personal Information (APPI) provides that a business operator handling personal information shall take necessary and proper measures for the prevention of leakage, loss, or damage, and for other security control of the personal data. As a matter of interpretation of this Article, the entity that committed a data breach may be legally obliged to notify individuals who may be affected by such data breach.

   Although notice to regulators is not obligatory, it may be required under guidelines. For example, the Financial Service Agency, which is in charge of financial transactions, has issued a guideline dated December 6, 2004 that requires providers of financial services to notify a data breach to affected individuals and the Financial Service Agency and also publish it without delay.

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?**

   This will depend on the relevant guidelines.

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?**

   Typically there are no specific requirements as to the contents and time period and method of notice under guidelines. Notice must be given or publication of the breach must be made without delay.

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

   There are no penalties or fines, but failing to notify will likely result in higher damages. Further, if an entity fails to make a report or makes a faulty report against report orders of competent government agencies, it will be subject to criminal penalties (a fine of JPY 300,000 or less).

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)?**

   Notification to each affected individual and to the public are recommended in order to minimize any possible damages.

6. **What are the applicable data protection laws or guidelines within your country?**

   The main data protection national laws and regulations:

   - Act on the Protection of Personal Information (APPI); and
   - As of July 29, 2010, 40 guidelines had been issued by various government agencies in relation to 27 business and other fields. No English translation is available.

7. **Contact information for Data Protection Authority:**

Name:	Consumer Affairs Agency (responsible for general legal framework only)
Address:	Sanno Park Tower, 11-1, Nagatacho 2, Chiyoda-ku, Tokyo, Japan
Telephone:	+81 3 5253 2111 or +81 3 3507-8800
Fax:	None available
Email:	None available
Website:	www.caa.go.jp

For more information, contact:

Name:	Tsuneo Sato
Firm:	City-Yuwa Partners
Address:	Marunouchi Mitsui Building, 2-2-2 Marunouchi, Chiyoda-ku, Tokyo, 100-0005
Telephone:	+ 81 3 6212 5502
Fax:	+ 81 3 6212 5700
Email:	tsuneo.sato@city-yuwa.com
Website:	www.city-yuwa.com

LUXEMBOURG

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)?**

   Except in the electronic communications sector, there is no legal obligation or requirement to notify the affected individuals. The operator and the service provider of electronic communications must inform the subscribers of any imminent risk of breach of the security of the network or services which may compromise the confidentiality of communications.

   There is no legal obligation or requirement to notify the DPA.

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?**

   The obligation to notify only applies to data held by electronic communications operators and service providers located in the territory of the Grand-Duchy of Luxembourg or to electronic communications operators and service providers who are not based on Luxembourg territory or the territory of any other Member State of the European Union but uses processing resources located on Luxembourg territory, apart from resources that are used only for the purposes of transit through the said territory or that of another European Union Member State. These obligations do not apply to a data controller in any other situation.

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?**

   There is no legal requirement regarding the content of the notice, time period in which notice must be given, or method of giving notice. The law only indicates that the operator or the service provider of electronic communications must indicate the imminent risk of the breach of the security of the network or services and possible remedies, including an indication of the likely costs involved.

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

   In civil litigation, any person affected by a fault of a data controller would be entitled to obtain compensation for loss or damage. This person must prove the fault, the damage and link between the fault and the damage.

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)?

It is highly advisable to inform the data subjects in the event of data breaches that may affect their personal data even where there is no general mandatory obligation to notify an affected person.

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

The main data protection legislation is:

- The law of 2 August 2002 on the Protection of Persons with regard to the Processing of Personal Data; and
- The law of 30 May 2005 relating to Specific Provisions for the Protection of Persons with regard to the Processing of Personal Data in the electronic communications sector.

7. Contact information for Data Protection Authority:

Name:	*Commission Nationale pour la Protection des Données* (National Commission for Data Protection)
Address:	41, avenue du Rock'n'Roll, L-4361 Esch-sur-Alzette, Grand-Duchy of Luxembourg
Telephone:	+352 26 10 601
Fax:	+352 26 10 60 29
Email:	See website
Website:	www.cnpd.lu

For more information, contact:

Name:	Sophie Wagner-Chartier
Firm	Arendt & Medernach
Address:	14, rue Erasme, L-2082 Luxembourg
Telephone:	+352 40 78 78 253
Fax:	+352 40 78 04 701
Email:	sophie.wagner@arendt.com
Website:	www.arendt.com

MALAYSIA

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)?**

   No, there is no requirement to notify either individuals or the data protection authority. In addition, the Personal Data Protection Act 2010 (not yet in force) does not bring in such a requirement.

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?**

   Not applicable.

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?**

   Not applicable.

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

   Not applicable.

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)?**

   Generally yes but it is necessary to consider the nature and extent of the breach on a case by case basis.

6. **What are the applicable data protection laws or guidelines within your country?**

   The main data protection national laws and regulations are the following:

   - Personal Data Protection Act 2010 (not yet in force but expected to come into force in 2013); and
   - Credit Reporting Agencies Act 2010.

7. Contact information for Data Protection Authority:

Name:	Personal Data Protection Department
Address:	Level 6, Kompleks KPKK, Lot 4G9, Persiaran Perdana, Presint 4, Pusat Pentadbiran Kerajaan Persekutuan, 62100 Putrajaya
Telephone:	Noreen Iszani (+60 3 8911 7925) or Ahmad Syazwan (+60 3 8911 7920)
Fax:	+60 3 8911 7959
Email:	pcpdp@kpkk.gov.my
Website:	www.kpkk.gov.my (Malay only)

For more information, contact:

Name:	Raymond TC Low
Firm:	Shearn Delamore & Co.
Address:	7th Floor Wisma Hamzah Kwong Hing, No 1 Leboh Ampang, 50100 Kuala Lumpur, Malaysia
Telephone:	+60 3 2027 2839
Fax:	+60 3 2078 5625
Email:	Raymond@shearndelamore.com
Website:	www.shearndelamore.com

MEXICO

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)?**

   Pursuant to Article 20 of the Federal Law for the Protection of Personal Data in Possession of Individuals in Mexico ("Mexican Data Privacy Law") and Article 64 of the Regulations of the Mexican Data Privacy Law ("Regulations"), any security breach significantly affecting the financial and moral rights of the data subject shall be notified by the data controller to such data subject(s).

   The data subject does not need to be a national of Mexico, but only an individual who is considered as a data subject under the Mexican Data Privacy Law, therefore the Mexican Data Privacy Law may be applicable to a controller located outside of Mexico.

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?**

   The notification must be given by the controller upon the confirmation of the occurrence of any security breach at any stage of processing of the personal data (for example collection, use, disclosure, storage and transferring), and once the controller has taken any actions intended to analyse the extent of the breach.

   Mexican Data Privacy Law and its Regulations are not specific about the type of personal data that needs to be affected by a security breach to trigger the controller's obligation to give a personal data breach notice. Instead, they provide that any breach significantly affecting the financial or moral rights of the data subject should be notified.

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 terms of Article 65 of the Regulations the notice shall at least contain:

   - The nature of the incident;
   - The personal data affected;
   - Advice on the actions that may be adopted by the data subject to protect his/her interests;
   - Details of the remedial actions that were immediately carried out; and
   - The means through which the data subject may obtain further information.

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

   In a general sense and subject to an analysis on a case-by-case basis, failing to notify the data subject may be deemed by the Federal Institute for Information Access and Data Protection ("IFAI") as a breach of data privacy principles provided by the Mexican Data Privacy Law. Accordingly, the IFAI may impose a fine between 100 to 160,000 times the minimum wage in force in Mexico City (currently between $6,476.00 and $10,361,600.00 Mexican Pesos). The above would not prevent the data subject from exercising any action for indemnification under civil or criminal law, if any.

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)?**

   Depending on the type of breach and the personal data affected, we would recommend notifying a security breach even if it is not mandatory under the Mexican Data Privacy Law to reduce or limit any possible damage to the data subject that could result in a liability to the controller under civil or criminal law.

6. **What are the applicable data protection laws or guidelines within your country?**

   The main data protection national laws and regulations are:

   - Federal Law for the Protection of Personal Data in Possession of Individuals; and
   - Regulations of the Federal Law for the Protection of Personal Data in Possession of Individuals.

7. **Contact information for Data Protection Authority:**

Name:	Federal Institute for Information Access and Data Protection
Address:	Insurgentes Sur No. 3211 Colonia Insurgentes, Cuicuilco, Delegación Coyoacán, C.P. 04530
Telephone:	1 800 835 4324
Fax:	None available.
Email:	atencion@ifai.org.mx
Website:	www.ifai.org.mx

For more information, contact:

Name: César G. Cruz Ayala
Firm: Santamarina y Steta
Address: Torre ING, Batallón de San Patricio 111, Piso 11, Col. Valle Oriente, 66269 Garza García, N.L., (Monterrey) México
Telephone: +52 81 8133 6000 or Direct Dial +52 81 8133 6002
Fax: +52 81 8368 0111
Email: ccruz@s-s.mx
Website: www.s-s.mx

NETHERLANDS

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)?**

   To date, there is only a limited generic data breach notification duty. The Personal Data Protection Act ("PDPA") requires data controllers to provide data subjects with information, where this is necessary in the circumstances in order to guarantee that the processing is carried out in a proper and careful manner (article 6 and 33 PDPA). According to this rule, data subjects must be notified of a breach that concerns their data.

   In addition there are certain sector-specific legal requirements

   - *Telecoms*: providers of publicly available electronic communications services must notify the Dutch telecoms authority ("OPTA") of all incidents where personal data has been put at risk. Affected individuals must be notified as well, unless appropriate technical security measures have been taken to encrypt the personal data involved, or otherwise render the data incomprehensible.
   - *Banking*: under the Financial Services Act, banks and other financial institutions must report incidents to the Nederlandsche Bank and The Netherlands Authority for the Financial Markets (AFM).

   The Dutch government has proposed a new act that introduces a data breach notification duty on all data processors, but to date this bill has not been enacted. This new act will amend the PDPA and imposes a notification duty on all data processors that discover a data breach.

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?**

   The general duty to notify only applies to data controllers and is not limited to specific types of personal data. The data subjects only have to be notified if, considering the types of personal data that were lost and the nature of the data breach, information in respect of the data breach is relevant for the data subject. For instance, if passwords were obtained by hackers, the data subjects would have to be informed and recommended to change their passwords.

   - *Telecoms*: This notification applies to any breach that has adverse consequences for the protection of personal data processed in connection with the provision of a publicly available electronic communications service in the European Union. It is not limited to specific types of data and all providers of publicly available electronic communications

services are subjected to this duty, regardless of whether or not they act as a data controller.

- *Banking*: This notification duty is worded in a very generic manner. If the incidents may affect the public's trust in the financial sector, the regulated financial institution will have to notify its regulatory authority. This will typically be the case if the incident concerns financial data of individuals and companies.

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?

No specific requirements are set out in the PDPA. The notification will generally have to take place in a manner and within a timeframe that is adequate to enable the data subjects to respond to the incident.

Telecoms: data breach notification under the regulations for the telecoms sector should be sent immediately (within 24 hours), normally online (or if this is not possible then by telephone) and must at least contain information about:

- The date on which the breach occurred;
- The type of data breach and information about the personal data;
- The estimated number of individuals involved;
- The risk of harm;
- Notification to the affected individuals; and
- Any steps that have been taken to reduce the risk of harm.

Under the Netherlands' new data breach notification act, the notifications should be sent immediately (within 24 hours), and will at least have to contain:

- The nature of the incident;
- Contact details of the officers who can provide more details re the reported incident;
- The recommended measures to reduce the risk of harm;
- A description of the adverse consequences identified and expected as result of the incident; and
- A description of the mitigating measures already taken by the data controller.

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

The DPA can impose administrative penalties up to €4,500 per violation.

- *Telecoms*: a penalty of up to €450,000 could be imposed;
- *Pending New Act*: with the enactment of the new data breach notification act, penalties amounting to a maximum of €200,000 per violation may be imposed.

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)?

Notification to the authorities is recommended and whether notification to the data subjects is appropriate will have to be assessed on a case-by-case basis. In order to reduce exposure it is advisable to discuss this with the competent regulatory authority (DPA or sector-specific authority).

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

The main data protection national laws and regulations are the following:

- Personal Data Protection Act ("*Wet bescherming persoonsgegevens*"), and
- Telecommunications Act ("*Telecommunicatiewet*").

7. Contact information for Data Protection Authority:

Name:	Dutch Data Protection Authority
Address:	Juliana van Stolberglaan 4-10, 2595 CL Den Haag, (The Hague)
Telephone:	+31 70 888 85 00
Fax:	+31 70 888 85 01
Email:	None available.
Website:	www.dutchdpa.nl

For more information, contact:

Name:	Wouter Seinen
Firm:	CMS Derks Star Busmann
Address:	Newtonlaan 203, 3584 BH Utrecht, The Netherlands
Telephone:	+31 30 2121 191
Fax:	+31 30 2121 157
Email:	wouter.seinen@cms-dsb.com
Website:	www.cms-dsb.com

NORWAY

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)**?

   Enterprises and businesses processing personal data may have a duty to notify the Norwegian Data Inspectorate in the event of a data breach.

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?**

   All enterprises and businesses processing personal data have a general duty of notification to the Norwegian Data Inspectorate if there has been a data breach that has led to an unauthorized distribution of personal data that should be treated confidentially.

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?**

   The Norwegian Data Inspectorate has provided guidelines that the notification should be given as soon as possible by telephone, letter or e-mail and should include:

   - A description of when and how the breach has occurred;
   - Who the affected individuals are;
   - What type of data has been breached;
   - What the enterprise/business has done to minimize damages;
   - What the enterprise/business will do to aid or assist the affected individuals; and
   - All relevant contact information.

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

   The Norwegian Data Inspectorate regularly issues fines for breaches on the applicable legislation (Personal Data Act and Personal Data Regulations). Pursuant to Norwegian law, fines may reach USD 140,000; however, recent practice indicates fines less than USD 50,000 even for continuous and serious breaches that involve processing of sensitive personal data. The authority normally issues a warning before issuing a fine. The data controller could also face a custodial sentence of maximum one year.

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)?**

   Yes, the Norwegian Data Inspectorate has stated that this is highly recommended in most instances, especially if the breach is considered to be serious.

6. **What are the applicable data protection laws or guidelines within your country?**

   The main legislation and regulations are the Personal Data Act of 14 April 2000 no 31 and Personal Data Regulations of 15 December 2000 no 1265.

7. **Contact information for Data Protection Authority:**

Name:	The Norwegian Data Inspectorate
Address:	P.O Box 8177 Dep, N-0034, Oslo, Norway
Telephone:	+47 22 39 69 00
Fax:	+47 22 42 23 50
Email:	postkasse@datatilsynet.no
Website:	www.datatilsynet.no

For more information, contact:

Name:	Halvor Manshaus
Firm:	Advokatfirmaet Schjødt AS
Address:	Ruseløkkveien 14, P.O.Box 2444 Solli, NO-0201 Oslo, Norway
Telephone:	+47 22 01 88 00
Fax:	+47 22 83 17 12
Email:	halvor.manshaus@schjodt.no
Website:	www.schjodt.no

PERU

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)?**

   Under Peruvian law, there is no legal obligation or requirement to notify either the affected individual or the DPA in the event of a data breach.

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?**

   Not applicable.

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?**

   Not applicable.

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

   There are no penalties, fines or risks in failing to notify.

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 some cases, for example credit card data breaches, notifying the affected individuals is recommended, in order to avoid being classified as a non-suitable service provider, according to Peruvian consumer protection laws.

6. **What are the applicable data protection laws or guidelines within your country?**

   The key legislation is the Peruvian Personal Data Protection Act (Ley 29733, Ley de Protección de Datos Personales).

7. Contact information for Data Protection Authority:

Name:	Autoridad Nacional de Protección de Datos Personales
Address:	Calle Scipión Llona N° 350, Miraflores
Telephone:	+511 204 8020 ext. 1213
Fax:	None available
Email:	andp@minjus.gob.pe
Website:	www.minjus.gob.pe/proteccion-de-datos-personales

For more information, contact:

Name:	Carlos A. Patrón or Julio Reyes Flores
Firm:	Payet Rey Cauvi Abogados
Address:	Av. Víctor Andrés Belaúnde 147, Centro Empresarial Real, Torre Real Tres Piso 12, San Isidro, Lima 27, Perú
Telephone:	+511 612 3202
Fax:	+511 222 1573
Email:	cap@prc.com.pe or jrf@prc.com.pe
Website:	www.prc.com/pe

PHILIPPINES

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)?**

   No, notice to the affected individual (the data subject) or the National Privacy Commission (DPA) is not required, except for in exceptional circumstances as detailed in the answer to question 2 below.

   The National Privacy Commission has not yet been established: however, the answer to question 2 below sets out how notification should be made.

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?**

   Pursuant to Republic Act No. 10173 (Data Privacy Act of 2012), Section 20(f), notice to the National Privacy Commission and the affected individual is required when sensitive personal information or other information that may, under the circumstances, be used to enable identity fraud is reasonably believed to have been acquired by an unauthorised person, and the personal information controller or the National Privacy Commission believes that such unauthorised acquisition is likely to give rise to a real risk of serious harm to any affected data subject. Section 3(l) of the Data Privica Act states that sensitive personal information refers to personal information:

   - About an individual's race, ethnic origin, marital status, age, colour, and religious, philosophical or political affiliations;
   - About an individual's health, education, genetic or sexual life, or to any proceeding for any offense committed or alleged to have been committed by such person, the disposal of such proceedings, or the sentence of any court in such proceedings;
   - Issued by government agencies particular to an individual which includes, but is not limited to, social security numbers, previous or current health records, licenses or denials of such, suspension or revocation, and tax returns; and
   - Specifically established by an executive order or an act of Congress to be kept classified.

   The entity has to be a personal information controller.

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?**

Notification should give a description of the nature of the breach, the sensitive personal information possibly involved, and the measures taken by the entity to address the breach and should be given as soon as possible. Notification may be delayed only to the extent necessary to determine the scope of the breach, to prevent further disclosures, or to restore reasonable integrity to the information and communications system.

While there is no prescribed method of notification provided in the Data Privacy Act of 2012 (and the rules and regulations to implement the law have not yet been issued), it is advisable that notice should at least be in writing, to enable the person giving notice to easily establish that he/she has given notice, and considering that the form of the consent of the data subject has to be in writing. Based on the Electronic Commerce Act of 2000, an email or an SMS is considered to be in writing.

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

Anyone who fails to inform the National Privacy Commission, after becoming aware of a security breach and of the obligation to notify the National Privacy Commission, and who intentionally or by omission conceals the fact of such a security breach according to section 30 of the Data Privacy Act is liable to imprisonment of between one year and six months to five years, and a fine of not less than Php500,000 but not more than Php1,000,000.

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)?**

Yes, section 6 of the Data Privacy Act of 2012 states that the Act has extraterritorial application when:

- The personal information of Philippine citizens or residents are processed; and
- The entity has a link with the Philippines such as when:

(a) A contract is entered in the Philippines, or

(b) A juridical entity unincorporated in the Philippines but has central management and control in the country, or

(c) An entity that has a branch, agency, office or subsidiary in the Philippines and the parent or affiliate of the Philippine entity has access to personal information; and

- The entity has other links in the Philippines such as when:

(a) The entity carries on business in the Philippines, or

(b) The personal information was collected or held by an entity in the Philippines.

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

The key legislation is:

- Republic Act No. 10173 (Data Privacy Act of 2012), which was enacted on August 15, 2012, on personal information;
- Republic Act No. 8792 (Electronic Commerce Act of 2000) on data message and electronic document; and
- Special laws such as Republic Act No. 2382 (Medical Act of 1959) Section 24 (12), Republic Act No. 8504 (AIDS Prevention and Control Act) Section 30, and Republic Act No. 7277 (Magna Carta of Disabled Persons) Section 33 may also apply.

7. Contact information for Data Protection Authority:

This is not yet available. Although the Data Privacy Act of 2012 created the National Privacy Commission under the Office of the President and made available the appropriated funds, the National Privacy Commission has not yet been put in place.

For more information, contact:

Name: Rolando V. Medalla, Jr. or Hiyasmin L. Lapitan or Ma. Luisa D. Manalaysay
Firm: SyCip Salazar Hernandez & Gatmaitan
Address: SyCipLaw Center, 105 Paseo de Roxas, Makati City 1226, The Philippines
Telephone: +63 (2) 982 3500 or +63 (2) 982 3600, or +63 (2) 982 3700
Fax: +63 (2) 817-3145 or +63 (2) 817 3896
Email: rvmedalla@syciplaw.com or hhlapitan@syciplaw.com
or mldmanalaysay@syciplaw.com
Website: www.syciplaw.com

PORTUGAL

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)?**

   In Portugal, the only data breach notifications that are legally required concern electronic communication providers. According to Law no. 46/2012, of 29 August, which implemented the changes introduced by Directive 2009/136/EC to Directive 2002/58/EC, and concerns the processing of personal data and the protection of privacy in the electronic communications sector (the "Communications Privacy Law"), if there is a risk that the breach will adversely affect the personal data (for example, because it presents a risk of identity fraud, physical injuries, humiliation, damage to the individual's reputation), the subscriber or individual whose data could be affected must be notified by the electronic communications service provider.

   This notification obligation will not apply if the companies offering publicly available electronic communications services are able to prove to the *Comissão Nacional de Protecção de Dados* ("CNPD") that they have taken the necessary technological protection measures and that these measures were applied to the data breached.

   The Communications Privacy Law also requires companies that offer electronic communication services to notify the CNPD whenever there is a personal data breach.

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?**

   In order to trigger notification, the data breach must concern personal data, which is broadly defined by Law 67/98, of 26 October (the "Data Protection Law") as any kind of information, regardless of its support, including sound and image, concerning an identified or identifiable person.

   Whenever personal data is processed by an electronic communications service provider (such as internet service providers and telecom operators) during the course of its business of providing electronic communications services and a breach takes place, the notification obligation is triggered.

   The obligation of notification is only imposed on companies that offer electronic communications services accessible to the public. As the Communications Privacy Law does not distinguish between controllers and processors, all electronic communications service providers must notify the CNPD in case of a data breach.

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?**

The content of the notification depends on its addressee: the notifications to the data breach-affected individuals must contain, as their minimum elements, the identification of the nature of the personal data breach and the contact points where additional information can be obtained, as well as the recommendation of measures designed to mitigate any adverse effects deriving from the breach.

The notifications to the CNPD must contain, in addition to the minimum elements referred to in the preceding paragraph, the consequences of the breach of personal data and the identification of the measures proposed or taken by the company offering publicly available electronic communications services to counteract the breach.

Both the notifications to the affected individuals and to the CNPD must occur "without unjustified delay" and the law does not provide for a specific method of giving notice but empowers the CNPD to, in accordance with the decisions of the European Commission, issue guidelines or instructions concerning the circumstances in which companies that offer publicly available electronic communications services are required to notify the personal data breaches, as well as on the form and procedure applicable to those notifications.

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

Whenever the CNPD verifies that the obligation of notification has not been complied with, it shall notify the offender of such fact and give it the opportunity to respond within a minimum period of 10 days and, where applicable, terminate the non-compliance.

Non-compliance with the notification requirements amounts to an administrative offense punishable with a fine ranging from a minimum of €500 Euro and a maximum of €20,000, when the defaulter is an individual, and from a minimum of €2,500 and a €2,500,000 when it is legal entity that breaches the duty. It is up to the CNPD to commence, investigate and close this process as well as to impose the respective fine.

Nevertheless, compliance with the sanction does not exempt the defaulter from having to comply with the duty of notification, if this is still feasible. If the defaulter does not comply with the decision of the CNPD, the latter may impose a periodic penalty payment of which the daily value may range, depending on the economic situation of the defaulter and the default's negative impact on the market, between €50 and €100,000.

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)?**

   It is recommended to notify individuals if the breach creates a risk of harm, as this will generally allow individuals to take steps to minimize such harm.

6. **What are the applicable data protection laws or guidelines within your country?**

   The main data protection national laws and regulations are:

   - Law 67/98, of 26 October – Data Protection Law (implementing Directive 95/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data); and
   - Law 46/2012, of 29 August – "Communications Privacy Law" (implementing Directive 2009/136/EC of 25 November 2009 in the part that it amends Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector).

7. **Contact information for Data Protection Authority:**

Name:	Comissão Nacional de Protecção de Dados (CNPD)
Address:	Rua de São Bento, 148, R/C, 1200-821 Lisboa, Portugal
Telephone:	+351 21 392 8400
Fax:	+351 21 397 6832
Email:	geral@cnpd.pt
Website:	www.cnpd.pt

For more information, contact:

Name:	Daniel Reis
Firm:	PLMJ – Sociedade de Advogados, RL
Address:	Lisboa Av. da Liberdade, 224, Edifício Eurolex, 1250-148 Lisboa, Portugal
Telephone:	+351 21 319 7300 or direct dial +351 21 319 7313
Fax:	+351 21 319 7400
Email:	daniel.reis@plmj.pt
Website:	www.plmj.com/en

RUSSIA

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)?**

   No, currently there is no legal obligation to notify. However, the personal data processor is required to immediately take the necessary measures in order to remedy the effects of a data breach.

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?**

   Not applicable.

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?**

   Not applicable.

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

   Not applicable.

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)?**

   Depending on the nature of the breach and the nature of the data concerned, it might be advisable to notify the individuals, since the data processor is required to restore the personal data that was modified or deleted as a result of a data breach. In addition, proper and timely notification of the individuals may help to prevent greater damage caused by a data breach.

6. **What are the applicable data protection laws or guidelines within your country?**

   The key legislation is Federal Law No. 152-FZ "On Personal Data" dated 27 July 2006.

   A recent Federal Law has been passed to amend a number of existing acts. It deals with the processing of personal data in different fields and introduces more detailed regulation on data protection. It does not introduce a legal obligation to notify in the event of a data breach.

7. Contact information for Data Protection Authority:

Name:	The Federal Service for Supervision in the Sphere of Telecom, Information Technologies and Mass Communications (*Roskomnadzor*)
Address:	Kitaygorodsky proezd, 7, building 2, Moscow, 109074, Russia
Telephone:	+7 495 987 6750
Fax:	+7 495 987 6801
Email:	rsoc_in@rsoc.ru
Website:	www.rsoc.ru

For more information, contact:

Name:	Maxim Boulba
Firm:	CMS, Russia
Address:	Gogolevsky Blvd. 11, 119019 Moscow, Russia
Telephone:	+7 495 786 4000
Fax:	+7 495 786 4001
Email:	maxim.boulba@cmslegal.ru
Website:	www.cmslegal.ru

SERBIA

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)?**

   There is no legal obligation to inform the affected individuals or the Serbian Data Protection Authority.

   However, if the data breach has elements of a criminal offense (e.g. unauthorized collection of personal data, unauthorized access to a computer or computer network, etc.), under the provisions of the criminal law, the police must be notified. In case the Serbian Data Protection Authority learns of such a data breach it has the obligation to notify the police.

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?**

   Not applicable.

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?**

   Not applicable.

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

   Not applicable

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

   The notification to individuals may be recommended in the event of a data breach.

6. **What are the applicable data protection laws or guidelines within your country?**

   - Personal Data Protection Law ("Official gazette of RS", Nos. 97/2008, 104/2009, 68/2012 and 107/2012); and
   - Law on the Ratification of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data ("Official gazette of FRY – International treaties", No. 1/92, "Official gazette of Serbia and Montenegro - International treaties", No. 11/2005, "Official gazette of RS - International treaties", Nos. 98/2008 and 12/2010).

7. Contact information for Data Protection Authority:

Name:	*Poverenik za informacije od javnog značaja i zaštitu podataka o ličnosti*
Address:	Deligradska 16, 11000 Belgrade, Serbia
Telephone:	+381 11 340 8910
Fax:	+381 11 264 5647
Email:	office@poverenik.rs
Website:	www.poverenik.rs

For more information, contact:

Name:	Ksenija Ivetić or Radivoje Petrikić
Firm:	CMS Reich-Rohrwig Hasche Sigle d.o.o.
Address:	Cincar Jankova 3, Belgrade, SRB-11000, Serbia
Telephone:	+381 11 320 8900
Fax:	+381 11 303 8930
Email:	Ksenija.Ivetic@cms-rrh.com or Radivoje.Petrikic@cms-rrh.com
Website:	www.cms-rrh.com

SINGAPORE

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)?**

   No, Singapore's *Personal Data Protection Act 2012* (parts of which came into force on 2 January 2013) does not have any provision that requires that an affected data subject be notified. Neither does the Act require that the Personal Data Protection Commission be notified of such breaches. Neither does other Singapore legislation explicitly require data breach notifications to be provided to either the affected individuals or a regulator.

   However, it would be prudent for financial institutions regulated by the Monetary Authority of Singapore ("MAS") to notify the MAS of any data breach, since the data breach may have resulted from the financial institution not complying with MAS' Guidelines and/or Circulars (for example, Circular No. SRD TR 01/2009 "Endpoint Security and Data Protection").

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?**

   Not generally applicable, however in relation to financial institutions, which are usually data controllers and data processors, MAS Circular No. SRD TR 01/2009 ("Endpoint Security and Data Protection") specifically identifies "customer personal information, identity details and transaction data" as data that should be encrypted or protected prior to any transmission, dispatch or conveyance.

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?**

   Not generally applicable, however in relation to financial institutions, a MAS consultation paper in June 2012 proposed that any IT security incident be notified to the MAS in writing within 30 minutes of the discovery of the IT security incident. An "IT security incident" includes an event that involves, among other things, compromise of customer data. It is recommended that notifications should be made as soon as practicable.

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

   Not generally applicable in relation only to a failure to notify. However, under the *Personal Data Protection Act 2012*, a party in possession or control of personal data should protect such data by "making reasonable security arrangements to prevent unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks". A data breach may cause the Personal Data Protection Commission to be satisfied that the organisation has not complied with the aforementioned requirement and consequently direct the organisation to pay a financial penalty. The penalty may be of such amount as the Commission thinks fit but in any event, not more than €1 million. Further, any person who suffers loss or damage by reason of the organisation not complying with the aforementioned requirement may bring a civil suit against the organisation and if the claim is made out, the court may grant that person an injunction, declaration, damages or such other relief as the court may think fit.

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 light of the answer to question 4 above, it is recommended that notification be made together with remedial action and mitigation steps. The organisation may rely on those actions and mitigating steps to argue for a lower financial penalty or lower civil damages.

6. **What are the applicable data protection laws or guidelines within your country?**

   The main data protection national laws and regulations are the following:

   - *Personal Data Protection Act 2012*; and
   - Sectoral codes and guidelines such as Guidelines and Circulars issued by the MAS for financial services entities and sections of the "Code Of Practice For Competition In The Provision Of Telecommunication Services 2012" dealing with End User Service Information.
   - Parts III to VII of the *Personal Data Protection Act 2012* (dealing with the collection, use and disclosure of personal data and the enforcement of the provisions of the Act) are currently not in force but it is expected that these Parts of the Act will come into force approximately in mid-2014.

7. Contact information for Data Protection Authority:

Name:	Personal Data Protection Commission
Address:	None available
Telephone:	+65 6377 3131
Fax:	+65 6273 7370
Email:	info@pdpc.gov.sg
Website:	www.pdpc.gov.sg

For more information, contact:

Name:	Gilbert Leong
Firm:	Rodyk & Davidson LLP
Address:	80 Raffles Place, #33-00 UOB Plaza 1, Singapore 048624
Telephone:	+65 6225 2626 or direct dial +65 6885 3638
Fax:	+65 6225 1838
Email:	gilbert.leong@rodyk.com
Website:	www.rodyk.com

SLOVAKIA

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)?

Current Act on Personal Data Protection

The requirement to notify of a breach of personal data is described in Act. No. 428/2002 Coll. on personal data protection ("Act on Protection of Personal Data" or "the Act") as being among the duties of a personal data officer who is responsible for supervising compliance with the statutory provisions regarding the processing of personal data and the rights of the relevant data subjects.

The Act requires that a personal data officer must be appointed in organisations employing more than five people and must notify the controller in writing without undue delay of any breach of the statutory provisions of the Act in the course of the processing of personal data. If, after notification, the controller fails to rectify the situation without undue delay, the personal data protection officer shall notify the Office for Personal Data Protection of the Slovak Republic (the DPA, hereafter the OPDA).

If a data subject suspects that his/her personal data is being processed without authorisation, he/she may notify the OPDA of it.

Further, the Act gives the data subject the right to report his/her suspicion of a breach of the obligations or conditions stipulated by the Act. The notification shall be submitted to the OPDA in writing. Apart from the data subject, the notification may also be filed by any natural person alleging that his/her rights under the Act were directly infringed.

The illegal handling of personal data is considered to be a criminal offense.

New Act on Personal Data Protection

In addition, under the new Act (expected to come into force 1 July 2013), a processor, who is processing personal data on behalf of a data controller, has to notify the controller in writing, without undue delay, of any breach of statutory provisions of the Act. If after such notification, the controller fails to rectify the situation without undue delay, the processor must notify the OPDA of the breach.

If incorrect or incomplete personal data is provided to a recipient third party, or data is provided without legal right to do so, the controller must notify the recipient.

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?

Current Act on Personal Data Protection

In case of the mandatory notification of breach, the notification must be given by the personal data official of the controller. The type of data involved in the breach is not relevant; every breach must be notified.

The data subjects also have the right to notify of any data breach. Again, the type of data involved is not relevant.

New Act on Personal Data Protection

In addition, the new Act requires that mandatory notification of breach must be given by the processor. Again, the type of data is not relevant; every breach must be notified.

In the case of mandatory notification of incorrect, incomplete or otherwise faulty personal data to a third party, or the illegal provision of data, the notification duty will apply to controller.

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?

The content of the notice must contain:

a) The name, surname, address of the permanent residence and signature of the person giving the notification;

b) Identification of the person against whom the notification is filed; corporate name or name and surname, registered office or permanent residence, or corporate form and identification number;

c) The subject of notification stating which rights were violated by the processing of personal data;

d) Evidence supporting the allegations stated in the notification;

e) A copy of any document proving that the data subject has notified the breach to the data controller.

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

Under the current Act, the OPDA may impose a fine ranging from €996 to €99,582.

Under the new Act, the OPDA may impose:

- A fine ranging from €300 to €6,500 in cases in which the controller did not notify third parties to which he/she had provided incorrect, incomplete or otherwise faulty personal data;
- A fine ranging from €150 to €3,500 in cases in which the data controller official did not inform the controller or the OPDA about a breach of the Act;
- A fine ranging from €1,000 to €80, 000 in cases in which the processor did not inform the controller or the OPDA about a breach of the Act.

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

We would recommend the notification of such breach.

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

Act. No. 428/2002 Coll. on Personal Data Protection

Also in preparation are guidelines regarding the extent of security measures, and duties of the data protection official.

7. Contact information for Data Protection Authority:

Name:	The Office for Personal Data Protection of the Slovak Republic
Address:	Hraničná 12, 820 07, Bratislava 27, Slovak Republic
Telephone:	+421 2 3231 3214
Fax:	+421 2 3231 3234
E-mail:	statny.dozor@pdp.gov.sk
Website:	www.dataprotection.gov.sk/buxus/generate_page.php?page_id=92

For more information, contact:

Name:	Hana Supeková
Firm:	Ružička Csekes, in association with CMS
Telephone:	+421 2 3233 3444
Email:	hana.supekova@rc-cms.sk
Website:	www.rc-cms.sk

SLOVENIA

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)?**

   In general the Personal Data Protection Act (*Zakon o varstvu osebnih podatkov; ZVOP-1*; hereinafter: PDPA) does not prescribe an obligation on the data controller or any other party to inform either the affected individual or the regulator ("Slovenian Information Commissioner") if any (personal) data breach is detected.

   If, however, the data breach constitutes a criminal offence which is an abuse of personal data under the Slovenian Criminal Code (*Kazenski zakonik; KZ-1*), and if such is detected by a public authority, the latter is obliged to file a criminal denunciation with the prosecution authorities.

   Nonetheless, if the data breach occurs in connection with a publicly available electronic communication service, the provider of the public electronic communication services must inform the Agency for Communication Networks and Services of the Republic of Slovenia ("Communications Agency") of such breach and, if the breach may harm the privacy of the individual, also the respective individual. The Electronic Communications Act (*Zakon o elektronskih komunikacijah; ZEKom-1* or "ECA") however, provides exceptions to this rule.

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?**

   The law (PDPA, ECA, The Criminal Code) regulates the protection of the personal data. Personal data is any data relating to an individual, irrespective of the form in which it is expressed. The eventual breach relates to the personal data under the above definition.

   As the formal notification only applies in case of a breach through a publicly available electronic communication service (as described above), the notifying entity is the provider of the public electronic communication services, who has also notified the regulator on the intended services. The notification of the Communications Agency is obligatory irrespective of the severity of the breach while the affected individual must only be informed if the breach is likely to harm his/her personal data or privacy. If however the service provider proves to the Communications Agency that adequate technical security measures were adopted for the respective data, the described notification of the affected individual is not required.

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?**

   The content of the notice is only prescribed in case of a breach through the publicly available electronic communication service. In such case, the notification to the affected individual must contain the description of the data breach, contact data for further information and the suggested measures to mitigate eventual harmful consequences of the data breach. The notification to the Communications Agency must also contain a description of the consequences of the data breach and the suggested or undertaken measures due to the breaches.

   The notification to the Communications Agency should be made "promptly" and the notification to the affected individual "without unnecessary delay".

   The method of the notice is not prescribed. So far the corresponding regulatory act in that respect has not yet been adopted by the Communications Agency.

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

   A failure to denounce a criminal offence of an abuse of personal data that was detected by a public official may result in disciplinary action being taken against the public official and, in severe cases, also criminal liability.

   A failure to notify of a breach through the publicly available electronic communication service may result in a fine from €50,000 to €400,000 for the service provider as a legal entity and a fine from €500 to €10,000 for the legal representative of such legal entity. Single entrepreneurs may meet a lower fine.

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

   We would recommend notifying a security breach even when there is no express legal requirement for such, in order to comply with internationally recognized data privacy principles and standards.

   In the event of credit cards data breaches, banks in Slovenia are, pursuant to the Banking Act (*Zakon o bančništvu; ZBan-1*), only obliged to protect confidential information on the principle level. Nevertheless, most banks do prescribe in their General Terms and Conditions a specific obligation to notify an individual (e.g. via a text message) in the event of a credit card data breach.

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

The applicable laws and guidelines are the Personal Data Protection Act (*Zakon o varstvu osebnih podatkov; ZVOP-1*) and Electronic Communications Act (*Zakon o elektronskih komunikacijah; ZEKom-1*) together with their regulatory acts, as well as the Slovenian Criminal Code (*Kazenski zakonik; KZ-1*).

The Information Commissioner is empowered to issue binding decisions and non-binding opinions, and to adopt guidelines.

7. Contact information for Data Protection Authority:

The primary contact and authority for further information on data protection issues in Slovenia is:

Name:	Information Commissioner (*Informacijski pooblaščenec*)
Address:	Zaloška cesta 59, p.p. 78, SI-1000 Ljubljana, Slovenia
Telephone:	+386 (0) 1 230 97 30
Fax:	+386 (0) 1 230 97 78
Email:	gp.ip@ip-rs.si
Website:	www.ip-rs.si/?id=195

The notification authority for detected data breaches through the publicly available electronic communication service is:

Name:	Communication Networks and Services of the Republic of Slovenia (*Agencija za komunikacijska omrežja in storitve Republike Slovenije*), which until the full implementation of the Communications Act, is still called the Post and Electronic Communications Agency of the Republic of Slovenia (*Agencija za pošto in elektronske komunikacije Republike Slovenije*)
Address:	Stegne 7, SI-1000 Ljubljana, Slovenia
Telephone:	+386 (0) 1 583 63 00
Fax:	+386 (0) 1 511 11 01
Email:	info.box@apek.si
Website:	www.apek.si/apek-ang

For more information, contact:

Name:	Luka Fabiani
Firm:	CMS Reich-Rohrwig Hainz
Address	Bleiweisova 30, SI-1000 Ljubljana, Slovenia
Telephone:	+386 (1) 620 5210
Fax:	+386 (1) 620 5211
Email:	Luka.Fabiani@cms-rrh.com
Website:	www.cms-rrh.com

SOUTH KOREA

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, according to the *Personal Information Protection Act* (PIPA) and the *Act on Promotion of Information and Communications Network Utilization and Information Protection* (IT Network Act), the affected individuals must be notified of any data breach.

   The relevant regulators must also be notified of the data breach. These regulators may, depending on the particular facts of each instance, be the Ministry of Public Administration and Security (MOPAS), the Korea Internet Security Agency (KISA), the National Information Security Agency (NIA), or the Korea Communications Commission (KCC). However, in instances where the PIPA applies, the duty to report to the relevant regulator arises only if the number of the affected individuals in each case is at least 10,000.

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?**

   Under the PIPA, the notification duties arise when the data breach occurs. As mentioned in the answer to question 1 above, however, no notification or reporting is required where the minimum threshold number of the affected individuals is not met. Under the IT Network Act, the notification duties are triggered upon the occurrence of any data loss, theft or leakage affecting the "Personal Information" of a data subject.

   Personal information is defined under the PIPA as data that pertains to a living person, such as the name, resident registration number, images, by which the individual in question may be identified, (including information by which the individual in question cannot be identified but can be identified through simple combination with other information).

   Any entity or individual handling personal information files for the purpose of work, regardless of whether in the public or private sector, has a duty of notification to the relevant regulator.

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?**

   Notification in the case of a data breach, both under the PIPA and the IT Network Act, should include items of the breached personal information, when and how the breach occurred, the information on the means that are available to the affected individuals to minimize damage, the remedial steps planned by the data handler, and the relevant contact information of the data handler. The notification should be given without delay and can be given by regular letter, e-mail, fax or telephone.

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

   Any negligent failure to notify the regulator(s) is subject to a fine not exceeding KRW 30 million (about USD 30,000). In civil litigation, any person affected by the breach of personal data would be entitled to monetary compensation for loss or damage, which can vary in amount on a case-by-case basis.

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)?**

   Not applicable.

6. **What are the applicable data protection laws or guidelines within your country?**

   Korea enacted a general and comprehensive data protection law called the *Personal Information Protection Act* in March 2011, which applies to both the private and public sectors. Aside from the PIPA, the most prominent Korean data protection law is the IT Network Act, which is applicable as between IT service provider and its users.

7. **Contact information for Data Protection Authority:**

Name:	MOPAS (Ministry of Public Administration and Security)
Address:	209 Sejong-daero (Sejong-ro), Jongno-gu, Seoul, Korea
Telephone:	+82 2 2100 3399
Fax:	None available
Email:	None available
Website:	www.mopas.go.kr

Name:	KISA (Korea Internet Security Agency)
Address:	Daedong B/D, Garak-dong 79-3, Songpa-gu, Seoul, Korea
Telephone:	+82 2 405 4118
Fax:	None available
Email:	None available
Website:	www.kisa.or.kr

Name:	NIA (National Information Security Agency)
Address:	NIA Bldg, 77, Mugyo-Dong, Jung-Gu, Seoul, Korea
Telephone:	+82 2 2131 0114
Fax:	None available
Email:	None available
Website:	www.nia.or.kr

Name: KCC (Korea Communications Commission)
Address: KCC 178, Sejong-daero, Jongno-gu, Seoul, Korea
Telephone: +82 2 750 1114
Fax: None available
Email: None available
Website: www.kcc.go.kr

For more information, contact:

Name: Kang, Taeuk
Firm: Bae, Kim and Lee LLC
Address: Hyundai Marine & Fire Insurance Bldg. 17F, 137 Teheran-ro, Gangnam-gu, Seoul
Telephone: +82 2 3404 0485
Fax: +82 2 3404 0001
Email: taeuk.kang@bkl.co.kr
Website: www.bkl.co.kr

SPAIN

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)?**

   No, there is no obligation to notify the affected individuals. Under the Regulation referred to in the answer to question 6 below, all incidents that put personal data at risk should be registered in a "Security Breach Record" that the company must keep available for the DPA.

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

   Not applicable.

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?**

   The "Security Document" referred to in question 1 above is an internal document describing all security measures implemented for the information systems and databases, which must be drawn up and kept up to date by every controller and processor. This must be observed by all personnel having access to the personal data, the information system or to any support for relevant databases and should describe the procedure for reporting internally, and recording and handling incidents.

   Records must include data regarding the type of incident, the time it took place, the person who reports it, the person to whom the incident is reported, any effects of the incident, the corrective measures applied, the procedures put in place to recover data and the person(s) who carried out the process, the data restored and, if applicable, the identification of the data that has to be restored manually in a recovery process.

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

   Not applicable.

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

This would depend on the nature of the breach, including the type and volume of data involved, whether it is encrypted, whether the breach was a result of a deliberate act and the type of data subjects.

When the data controller is established in Spain, we recommend informing the DPA of the data breaches, as then the DPA would be much more cooperative with the company than if it were to discover the data breach through a complaint or a report in the media.

When the controller is not established in Spain, it is recommended that the issue is appropriately handled from the beginning, by informing the individuals, instead of waiting to be sued by the data subjects particularly when the company must inform individuals about the same data breach in other jurisdictions.

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

The main national data protection laws and regulations are:

- *Organic Act 15/1999, of December 13, on the Protection of Personal Data*, and
- Royal Decree 1720/2007, of December 21, approving the Regulation implementing Organic Act 15/1999, of December 13, on the Protection of Personal Data.

7. Contact information for Data Protection Authority

Name:	Agencia Española de Protección de Datos,
Address:	C/ Jorge Juan 6, 28001 Madrid, Spain
Telephone:	+34 901 100 099
Fax:	+34 912 663 517
Email:	See website
Website:	www.agpd.es

For more information, contact:

Name:	Javier Aparicio
Firm:	Cuatrecasas, Gonçalves Pereira SLP
Address:	Calle Almagro, 9, 28010 Madrid, Spain
Telephone:	+34 915 247 620
Fax:	+34 915 247 655
Email:	javier.aparicio@cuatrecasas.com
Website:	www.cuatrecasas.com

SWEDEN

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)?**

   No, however providers of publicly available electronic communications services shall, without undue delay, inform the supervisory authority on privacy incidents. If the incident is likely to be detrimental to the data subjects, and if the supervisory authority requests, the data subjects must also be informed without undue delay.

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?**

   Not applicable.

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?**

   Not applicable.

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

   Not applicable.

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)?**

   A duty to notify individuals of a breach could, under certain circumstances, follow from the data controller's obligation to implement appropriate technical and organisational measures in order to protect the personal data.

   Such measures could be to inform the data subjects to change their password or procure other safety measures in order to avoid any further data breaches, or to limit the damages. Such duty to notify falls within the security obligations set out in the Swedish Personal Data Act.

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

The key legislation is the *Personal Data Act* (1998:204).

7. Contact information for Data Protection Authority:

Name:	Datainspektionen
Address:	Drottninggatan 29, plan 5, Box 8114, 104 20 Stockholm, Sweden
Telephone:	+46 08 657 61 00
Fax:	None available.
Email:	datainspektionen@datainspektionen.se
Website:	www.datainspektionen.se

For more information, contact:

Name:	Bobi Mitrovic
Firm:	Setterwalls
Address:	Sankt Eriksgatan 5, P.O. Box 11235, SE-404 25, Gothenburg, Sweden
Telephone:	+46 31 701 17 00
Fax:	+46 31 701 17 01
Email:	bobi.mitrovic@setterwalls.se
Website:	www.setterwalls.se

SWITZERLAND

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)?**

   No, the Swiss *Federal Data Protection Act* (FDPA) does not provide for an explicit obligation to notify individuals or the Federal Data Protection and Information Commissioner (FDPIC). However, an obligation to notify individuals may arise from:

   i) The principle that persons processing personal data have to observe the rules of good faith (Art. 4 para. 2 FDPA);

   ii) The general obligation to mitigate damages; or

   iii) The fact that the processing party has to implement measures that are necessary to ensure data security which might entail instructions to individuals following a data breach.

   This must be assessed on a case-by-case basis.

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?**

   There is no general rule detailing under what conditions notification must be given. It is more likely that a data controller will have to notify individuals in the event of a data breach than a data processor. However, the answer to question 1 above may, in principle, also apply to data processors.

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?**

   No, this depends on the circumstances and is mainly a question of practicality and effectiveness. There are no particular formalities required.

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

   Failing to notify in the event of a data breach may lead to liability for damage caused by such failure and to an administrative investigation (potentially followed by recommendations concerning the processing of data).

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 each case, the processing party has to evaluate whether the individuals can expect a notification in view of the principle of good faith, whether a notification can avoid considerable further damage or whether data security requires a notification.

6. **What are the applicable data protection laws or guidelines within your country?**

   The key legislation is the *Federal Data Protection Act* and the related ordinances.

7. **Contact information for Data Protection Authority:**

Name:	Federal Data Protection and Information Commissioner
Address:	Feldeggweg 1, CH 3003 Berne, Switzerland
Telephone:	+41 (0)31 322 43 95
Fax:	+41 (0)31 325 99 96
Email:	None available
Website:	www.edoeb.admin.ch

For more information, contact:

Name:	Dr. Robert G. Briner or Markus Kaiser
Firm:	CMS von Erlach Henrici AG
Address:	Dreikönigstrasse 7, 8002 Zurich, Switzerland
Telephone:	+41 44 285 11 11
Fax:	+41 44 285 11 22
Email:	robert.briner@cms-veh.com or markus.kaiser@cms-veh.com
Website:	www.cms-veh.com

TAIWAN

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, Article 12 of the *Personal Information Protection Act* of Taiwan (PIPA) provides that "when the personal information is stolen, disclosed, altered or infringed in other ways due to the violation of this Law, the government agency or non-government agency should notify the Party after an inspection." Therefore, the affected individuals should be notified accordingly. There is no legal obligation to inform the competent Authority of Data Protection.

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?**

   According to Article 12 of the PIPA, the notification must be given once the breach occurs. Furthermore, the definition of personal information is regulated in Article 2 section 1 of the PIPA which provides that "personal information denotes the name, date of birth, I.D. card number, passport number, characteristics, fingerprints, marital status, family, education, occupation, medical record, medical treatment, genetic information, sexual life, health examination, criminal record, contact information, financial conditions, social activities and other information which may be used to identify a natural person, both directly and indirectly."

   According to Article 8, 15, and 19 of the PIPA, data collectors and data processors are required to comply with PIPA. Therefore, both data collectors and data processors should notify affected individuals if they are aware that personal information, which they collect or control, is stolen, disclosed, altered or infringed in other ways due to the violation of PIPA.

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?**

   According to Article 22 of the Enforcement Rules of the PIPA, the content of the notice should include the fact that personal information has been infringed and what measures have been taken in response.

   A specific time period is not specified in relevant laws, but it is advisable to notify as soon as possible after taking measures in response to a breach.

   According to Article 22 of the Enforcement Rules of the PIPA, methods of giving notice shall be prompt written document, telephone, text message, email, facsimile, electronic record or other manners which will be sufficient to make or likely make the affected individual receive the notification. However, if the notification costs are disproportionate, in consideration of

the technical feasibility and privacy protection of the affected party, such notification may be made via internet, news media or other appropriate manner.

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

According to article 48 of the PIPA, where a non-government agency is in violation of Article 12 of the PIPA, it will be ordered by the competent authority to take corrective measures within a specified time period. If such measures are not taken within that period, an administrative fine of no less than NT$20,000 but no more than NT$200,000 should be imposed for each violation.

In addition, according to Article 28 of the PIPA, where a government agency should be found liable for damages due to violation of the PIPA, then the level of such damages will be decided by the court.

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)?

Not applicable.

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

The key legislation is the *Personal Information Protection Act* of Taiwan and the Enforcement Rules.

7. Contact information for Data Protection Authority:

Name:	The Data Protection Authority in Taiwan is the "Ministry of Justice"
Address:	NO. 130, Sec. 1, Chongqing S. Rd., Taipei, 10048, Taiwan
Telephone:	+886 2 2191 0189
Fax:	None available
Email:	See website
Website:	www.moj.gov.tw/mp095.html

For more information, contact:

Name:	Shuai-Sheng (Jackson) Huang or Chih-Hsun (Andre) Hung
Firm:	Formosa Transnational
Address:	13th Floor, Lotus Building, 136, Section 3, Jen Ai Road, Taipei, 106, Taiwan
Telephone:	+886 2 2755 7366
Fax:	+886 2 2755 6486
Email:	shuai-sheng.huang@taiwanlaw.com
Website:	www.taiwanlaw.com

UKRAINE

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)?**

   There are no legislative provisions establishing mandatory requirements to notify the personal data owner (individual) about the breach of his/her personal data rights.

   There is no legal requirement to inform the State Service of Ukraine on Personal Data Protection (the DPA) about a data breach. The law only provides for the right of the owner of the personal data (individual) to inform the DPA about the facts of the personal data breach affecting such individual and apply for his/her right's protection.

   At the same time, the DPA has the right to carry out investigations and inspections, and if the facts of a personal data breach are discovered, the infringers may be exposed to the relevant administrative sanctions, followed where necessary with enforcement of such sanctions through the court. Moreover, the individual has the right to inform law enforcement authorities (e.g., police department) of the personal data breach affecting the individual or to file lawsuits against the infringers (organisations or persons committing violation of the individual's personal data rights) in order to restore his/her breached rights and seek compensation of damages caused by the infringement.

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?**

   A breach of practically any personal data may trigger the notification. The Ukrainian legislation describes personal data as data about an individual who is identified or may be specifically identified. It includes, in particular, data on the person's nationality, education, marital status, religious beliefs, health condition as well as address, date and place of birth.

   Neither the data controller nor a data processor is under the obligation to notify. Only the affected individual has the right to notify the DPA. A notification from an individual about data breach may be sent to the relevant authorities (either the DPA or law enforcement authorities) in written form. It must be based on the facts of the personal data breach.

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?

The notification must describe the facts of the personal data breach and contain the relevant information about the type of personal data, its owner and infringer.

Since the notification is not mandatory, respectively no submission deadline is established. The notification can be sent to relevant authorities by the affected individual at any time.

However, penalisation of the infringer (as a result of the respective notification) and compensation of damages caused by the breach would be possible only within the respective statutes of limitations. Administrative sanction may be applied to the infringer no later than two months after the breach or after the exposure of the breach (in case of continuing violation). The respective term of limitation for application of criminal liability is five years. Compensation of damages through civil proceedings may be possible with application of standard three years of statute of limitation.

The notification should be sent by regular mail or filed directly with the relevant authority in written form.

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

Since no obligation to notify is established, penalties and fines are not provided for by the law.

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

Such notification to an individual may be recommended as a general courtesy, however only the subsequent notification by the relevant individual to the competent authorities may have legal effect and consequences.

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

- Law of Ukraine "On Personal Data Protection" # 2297-VI, dated 1 June 2009, as amended;
- Criminal Code of Ukraine # 2341-III dated 5 April 2001, as amended; and
- Code of Administrative Offences # 8073-X dated 7 December 1984, as amended.

7. Contact information for Data Protection Authority:

Name:	State Service of Ukraine on Personal Data Protection
Address:	15, Maryny Raskovoi Str., 02660 Kyiv, Ukraine
Telephone:	+380 44 517 6800 (Hotline: +380 04 541 0122)
Fax:	+380 44 517 6800
Email:	info@zpd.gov.ua

For more information, contact:

Name:	Maria Orlyk or Aleksey Yasinsklyy
Firm:	CMS Reich-Rohrwig Hainz TOV
Address:	19-B Instytutska, 5th Floor, 01021 Kyiv, Ukraine
Telephone:	+380 44 500 1710 or +380 44 500 1724
Fax:	+380 44 500 1716
Email:	maria.orlyk@cms-rrh.com or aleksey.yasinskyy@cms-rrh.com
Website:	www.cms-rrh.com

UNITED KINGDOM

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)?**

   There is no general requirement under the U.K.'s *Data Protection Act* to notify breaches to either affected individuals or the DPA.

   Certain sectors however (such as financial services and the public sector) have other sector-specific notification requirements with notifications usually to be made to the sector regulator.

   Providers of public electronic communications services (e.g. internet service providers, telecoms providers, etc.) must notify the DPA if there is a personal data security breach as required by the Privacy and Electronic Communications (EC Directive) Regulations 2003 (the "PECR").

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?**

   See the answer to question 1 above.

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?**

   Where a personal data breach occurs in an "electronic communications service", the service provider must comply with the PECR, without undue delay, and notify the breach to the U.K. Information Commissioner (the DPA). The notification must include: a description of the nature of the breach, a description of the consequences of the breach and a description of the measures taken or proposed to be taken by the provider to address the breach.

   In addition, service providers must keep a log recording:

   - The facts surrounding the breach;
   - The effect of the breach; and
   - Remedial action taken.

   Unless measures are in place that render the breached data unintelligible, service providers must also notify subscribers if the breach is likely to adversely affect their personal data or privacy. Such notice is to be given without undue delay and must provide details of the nature of the breach, the provider's contact details and suggestions on how to mitigate the breach.

The Information Commissioner recommends that the service provider submits its log of breaches on a monthly basis and by doing so avoids recording the information twice. The Information Commissioner considers this sufficient to meet the requirement to notify without unnecessary delay except if the breach is particularly serious. In that case, the breach must be notified to the DPA as soon as possible.

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

   The Information Commissioner can issue monetary penalties against data controllers of up to £500,000 for serious breaches of the Data Protection Act, enforcement notices, and undertakings. Before doing so, the Information Commissioner's Office must be satisfied that the contravention was serious and was of a kind likely to cause substantial damage or distress and that the data controller either: a) deliberately contravened the DPA; or b) knew or ought to have known that there was a risk the contravention would occur and that it would be likely to cause substantial damage or distress, but still failed to take reasonable steps to prevent it from happening.

   The Information Commissioner will commonly investigate potential breaches of the Data Protection Act by serving an information notice, requiring the relevant data controller to provide information about their personal data processing and information about the potential breach. In addition, under certain circumstances, the Information Commissioner may (with a warrant from the court) exercise powers of entry, inspection and seizure of documents and equipment. Individuals who suffer (i) damage or (ii) damage and distress as a result of a breach of the Data Protection Act are also entitled to seek compensation through the courts.

   The Information Commissioner may issue monetary penalties against an electronic communications service provider of up to £1,000 under PECR.

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)?**

   The Information Commissioner recommends in guidance that "serious breaches" should be notified (even though this is not a requirement of the Data Protection Act). Although what is meant by "serious breaches" is not defined in the Data Protection Act or in the Information Commissioner's guidance (although examples are provided), the potential harm to individuals is the overriding consideration. The extent of harm will depend on the volume and the sensitivity of the personal data.

6. **What are the applicable data protection laws or guidelines within your country?**

The key legislation is the *Data Protection Act 1998* and also the Privacy and Electronic Communications (EC) Directive Regulations 2003.

7. Contact information for Data Protection Authority:

Name:	Information Commissioner's Office
Address:	Wycliffe House, Water Lane, Wilmslow, Cheshire, United Kingdom SK9 5AF
Telephone:	+44 (0) 303 123 1113 or +44 (0) 1625 545 745
Fax:	+44 (0) 1625 24510
Email:	notification@ico.org.uk or informationgovernance@ico.org.uk.
Website:	www.ico.gov.uk

For more information, contact:

Name:	Kirsten Whitfield
Firm:	Wragge & Co
Address:	55 Colmore Row, Birmingham, B3 2AS England
Telephone:	+44 (0) 121 685 276
Fax:	+44 (0) 870 904 1099
Email:	Kirsten_Whitfield@wragge.com
Website:	www.wragge.com

UNITED STATES

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. The majority of U.S. states and certain industry-specific laws, regulations and guidance require notice to be provided to affected individuals in the event of a data breach. Fifty U.S. jurisdictions, including 46 states, the District of Columbia, Guam, Puerto Rico and the U.S. Virgin Islands, have enacted data breach notification laws applicable to affected individuals resident in such jurisdictions. (As of April 2013, the states that do not yet have such notification laws are Alabama, Kentucky, New Mexico and South Dakota.)

   In addition to such state data breach notification requirements, companies in certain industries, such as banking, credit unions, insurance, and health care, are also subject to certain state and federal industry-specific breach notification requirements. Compliance with federal industry-specific requirements may satisfy state breach notification requirements. Finally, U.S. federal and state governmental entities are subject to separate data breach notification requirements for breaches of data in their possession or data bases.

   Many of these laws also require that notice be provided to state and sometimes federal governmental authorities; however, the United States does not have a single data protection authority or even use that term. Many state breach notification laws require notice to specified state agencies (in most cases, the state attorney general). Companies in particular industries are also required to provide notice to state or federal industry regulators in the event of a breach.

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?**

   Although the data breach notification requirements of the various jurisdictions are similar, they contain significant variations. The application of the various laws is based on the state of residence of the individual whose data was compromised, and in many cases are not limited by the company's place(s) of business.

   Each state may have a different definition of what constitutes a breach that triggers notification requirements. For example, some jurisdictions require notification if there is unauthorised "access" to Personal Information as defined by applicable law, while others only require notification in the event of unauthorised "acquisition" of Personal Information. Certain jurisdictions only require notice where such information is not encrypted or a specific harm threshold has been met, while others do not have any such exemption.

In the U.S., categories of information about individuals that can be used for identity theft and fraudulent financial transactions are generally referred to as "Personal Information," although there is some slight variation in terminology across the states. Laws and regulations in the U.S. also vary from state to state, and between state and federal law, as to exactly what information comprises Personal Information for purposes of breach notification requirements. Generally, the definition requires both a name (first initial and last name often suffices), and some additional item of information that could be used to steal a person's identity or access his or her financial accounts (or, in some cases, healthcare information) without authorisation. Most states define Personal Information for breach notification purposes as an individual's name plus one or more of the following:

- Credit card number;
- Social Security number;
- Driver's license or government-issued identification card;
- Medical insurance identification number; or
- Financial account information;

or, depending on the law or regulation triggered:

- Other government identification information that could be used for identity theft; or
- Password and customer identification numbers that allow access to a financial account without a name.

In certain states, other information is sufficient to trigger breach notification requirements, such as an individual's name plus his or her date of birth.

Most U.S. breach notification requirements are not defined in terms of "data controllers" or "data processors," as those terms are not ones used in the U.S. legal system. It is the entity that owns, licenses, or maintains the Personal Information that is usually required to notify individuals and/or government agencies. If a third-party vendor or processor causes the breach, the third party is generally required to notify the entity that owns, licenses, or maintains the Personal Information. It is still generally the obligation of the data owner to provide notice to affected individuals and/or government agencies, although on occasion, the notification obligation can be delegated from the data owner to the third-party vendor where the vendor caused the breach.

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?

Yes. Certain of the state and industry-specific breach notification laws require specific content, timing, and method for providing notice to affected individuals and/or governmental agencies. The requirements vary depending upon applicable law, making it important for a company that is responding to a data breach to ascertain which jurisdictions' notice

requirements are triggered, and to identify the requirements of each of those jurisdictions as applied to the situation. With regard to content, certain states require, for example, a general description of the breach, the date of the breach, or the types of Personal Information subject to the breach. In contrast, Massachusetts law provides that notices to affected individuals may *not* include the nature of the breach.

With regard to timing, most states require notice "as soon as practicable and without unreasonable delay following discovery of the breach" or impose a similar requirement. Under certain state and industry-specific requirements, however, notice must be provided within a specific number of days, e.g., Florida, Ohio and Wisconsin require that notice be provided to affected individuals within 45 days of discovering the breach, while pursuant to California's healthcare breach notification requirement, agency and individual notices must be provided no later than five business days after discovery of a breach.

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

Governmental agencies may assess fines and other penalties for non-compliance with notification obligations, including delayed notification or failure to notify. In addition, breached entities may face class action lawsuits following a breach even when complying with breach notification obligations.

In cases involving credit card breaches, certain industry contractual rules require notification to the merchant, acquiring bank or credit card companies, which in turn can impose payment card industry (PCI-DSS) related fines and penalties issued by the credit card brands or associations.

A company's exposure to such fines, penalties and litigation following a breach increase where the company is found to have been operating out of compliance with applicable privacy and data security requirements, such as the Massachusetts Data Security Regulation (201 CMR 17.00) or the Payment Card Industry Data Security Standards (PCI-DSS). In addition, companies regulated by the U.S. Federal Trade Commission (FTC) are subject to FTC enforcement for unfair or deceptive acts or practices pursuant to Section 5 of the *Federal Trade Commission Act*. The FTC has brought enforcement actions against companies following breaches, interpreting "unfair acts or practices" to include failure to implement reasonable and appropriate data security to protect Personal Information, and "deceptive acts or practices" to include non-compliance with and/or inaccurate statements in company privacy policies.

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)?

As noted in the answer to question 2 above, U.S. legal terminology does not refer to a "data controller" or a "data processor", but there are so many breach notification requirements that

almost any breach of personally identifiable information, as defined, will likely require some sort of notification, in the absence of an exception. Even for breaches affecting residents of the four states that do not currently require notification to affected individuals (Alabama, Kentucky, New Mexico and South Dakota), notice may be recommended for companies doing business in Texas in light of a recent amendment to the Texas breach notification statute which requires companies that conduct business in Texas to notify residents of states that do not require breach notification.

In addition, the Division of Corporation Finance of the U.S. Securities and Exchange Commission (SEC) has issued guidance that identifies cyber risks and incidents as potential material information to be disclosed under existing securities law disclosure requirements and accounting standards applicable to publicly traded companies.

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

A list of U.S. states and links to their data breach notification laws is available at www.ncsl.org/programs/lis/cip/priv/breachlaws.htm.

Examples of industry-specific breach notification legislation, regulations and guidelines are set out below:

- Banking: Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notices, issued by the Office of the Comptroller of the Currency, Treasury, Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, and Office of Thrift Supervision, Treasury, interpreting section 501(b) of the Gramm-Leach-Bliley Act and Interagency Guidelines Establishing Information Security Standards.
- Credit Unions: Guidelines for Safeguarding Member Information promulgated by the National Credit Union Administration (12 C.F.R. 748 and Appendices).
- Insurance: Certain state insurance departments have promulgated regulations or issued guidance imposing specific breach notification requirements upon their licensees (e.g., insurance companies, producers or third party administrators) in addition to the general state breach notification requirements. *See, e.g.*, Connecticut Insurance Department Bulletin IC-25, August 18, 2010; Ohio Insurance Bulletin 2009-12; Rhode Island Insurance Division Regulation 107; Wisconsin Insurance Bulletin dated December 4, 2006.
- Health Care:

- Federal Health Insurance Portability and Accountability Act of 1996, ("HIPAA") (42 U.S.C. § 201 et seq.);
- Health Information Technology for Economic and Clinical Health ("HITECH") Act and implementing regulations, require notice to affected individuals, the U.S. Department of Health and Human Services ("HHS"), and in some cases, the media, in the event of a breach of protected health information ("PHI");

- Federal Trade Commission (the "FTC") Health Breach Notification Rule, 16 C.F.R. Part 318, requiring notification to affected individuals, the FTC and HHS, as applicable, by covered entities, business associates, and vendors of personal health records ("PHR") in the event of a data breach involving PHI or PHR; and
- Certain states impose specific notification requirements upon health care providers in addition to the general state breach notification requirements. For example, Cal. Health Safety Code § 1280.15 requires agency and individual notice within five business days of discovery.

We note that additional privacy and data security requirements not relating to breach notification *per se* exist under both state and U.S. federal law.

A number of the above requirements are discussed in Edwards Wildman Palmer LLP's comprehensive paper entitled "Everyone's Nightmare: Privacy and Data Breach Risks," regarding privacy, data security and breach notification requirements, exposures presented by data breaches, recent court decisions, and lines of insurance potentially impacted. Please visit the Edwards Wildman Privacy and Data Protection Group's website to view the most recent edition: www.edwardswildman.com/services/servicedetail.aspx?firmService=251.

7. Contact information for Data Protection Authority:

There is no data protection authority *per se* in the United States, but there are a number of relevant U.S. federal and state agencies, as referenced above, to whom notice may be required. These include, for example, the Federal Trade Commission, the Office of Civil Rights of HHS, and numerous state attorneys general. See response to question 6, above.

For more information, contact:

Name:	Mark E. Schreiber (Boston), Theodore P. Augustinos (Hartford) or Karen L. Booth (Hartford)
Address:	Edwards Wildman Palmer LLP 111 Huntington Avenue, Boston, MA 02199 or 20 Church Street, Hartford, Connecticut 06103
Telephone:	+1 617 239 0585 (M. Schreiber), +1 860 541 7710 (T. Augustinos) or +1 860 541 7714 (K. Booth)
Fax:	+1 617 316 8352 (M. Schreiber), +1 888 325 9082 (T. Augustinos) or +1 888 325 9526 (K. Booth)
Email:	mschreiber@edwardswildman.com or taugustinos@edwardswildman.com or kbooth@edwardswildman.com
Website:	www.edwardswildman.com