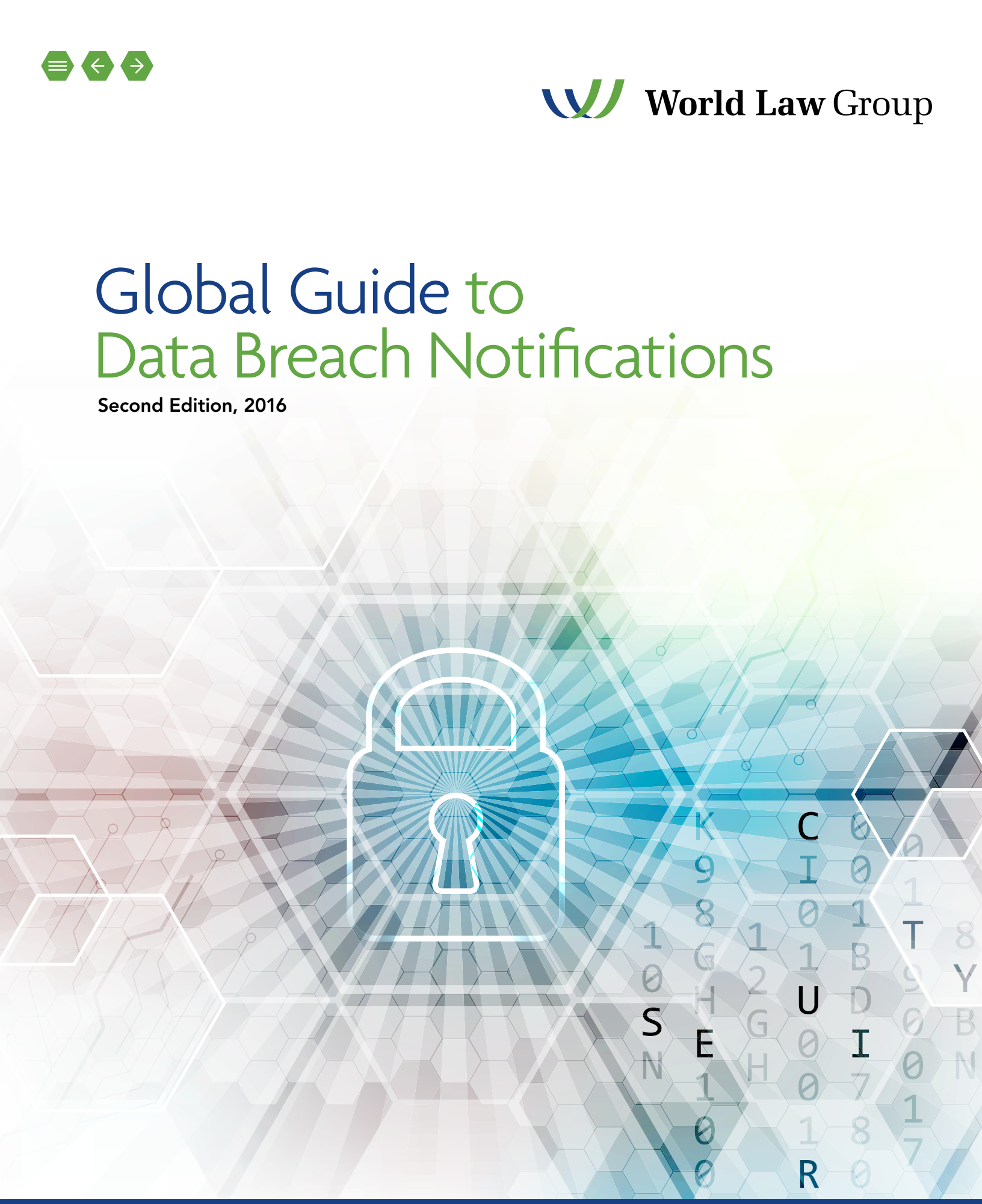
World Law Group

Global Guide to Data Breach Notifications

Second Edition, 2016



globaldatabreachguide.com

WORLD LAW GROUP GLOBAL GUIDE TO DATA BREACH NOTIFICATIONS, 2016

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 or offered 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. Legal counsel and advice should routinely be obtained, including locally for any particular jurisdiction. Please consult your own counsel.

This publication may constitute "Attorney Advertising" in some countries or jurisdictions.

CONTENTS

I. INTRODUCTION

Management of a security incident or data breach is a complex task, whether in one country or many. The number of countries with laws or rules governing data breaches has grown, even in the short interval since the original publication of this guide in 2013. The aim of this publication is to have a dedicated resource on this subject, distilling the experience of numerous World Law Group ("WLG") member firms into a single reference.

The breadth and extent of well-publicised security breaches and attacks in all business sectors is evident. A host of studies confirm that data breaches present a costly and significant exposure to companies, both monetary and reputational. This exposure sometimes can be minimized by a rapid, thoughtful and well-organized response to a breach, which now requires cross-border knowledge of notification and other relevant obligations. Examples of the need for such vigilance are countless.

A malware intrusion, in which the hackers are able to export credit card or financial information to an off-shore website, may compromise data about residents of a number of countries. Different systems or databases at a company may be attacked in various locations.

Identifying the relevant laws and regulations can be a challenge for the most experienced practitioners, privacy and 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 currently stem from common European directives and will be covered by the General Data Protection Regulation in the future. Various other countries are also instituting their own data breach reporting requirements.

This guide focuses on the laws around the world as they currently stand at the date of publication. However, change in this area is constant. Please visit www.globaldatabreachguide.com where we hope to post updates as they become available, and feel free to consult other reference sources. It takes an extraordinary amount of work to produce a publication of this sort. We hope readers find it useful.

Mark E. Schreiber
Chair, WLG Privacy & Data Protection Group
Locke Lord LLP
Boston, Massachusetts, U.S.A.
Email: mark.schreiber@lockelord.com
Tel: + 1 617 239 0585

Christian Runte
Co-Chair, WLG Privacy & Data Protection Group
CMS Germany
Munich, Germany
Email: christian.runte@cms-hs.com
Tel: + 49 89 238 07163

Note regarding European law

Please be aware that we have added a separate section on the European Union. In the future, personal data security breach laws in Europe will be harmonised. As of 2018, the EU General Data Protection Regulation will replace the current European Data Protection Directive (and implementing national laws). The personal data breach notification requirements will be stringent and penalties for non-compliance even more so (amounting to as much as 4% of global annual turnover). The Regulation will require mandatory notification of breaches to regulators within a very short time, 72 hours if feasible, and notification is to be accompanied by a raft of information. This is referenced in the individual EU country chapters of the guide.

Acknowledgments

This guide would not have been possible without the extraordinary contributions of many lawyers and others from a number of World Law Group member firms. Several individuals deserve special recognition for the painstaking effort and careful attention that such a global publication requires. For this edition, Sarah Haghdoust, a senior associate at CMS Germany in Munich worked tirelessly in the compilation and organisation of the various country contributions of the many WLG firms. Julie Engbloom, a partner at Lane Powell PC in Portland, Oregon, along with attorneys Laura L. Richardson, Cozette Tran-Caffee and Hans N. Huggler handled the legal review. Karen Booth, an associate at Locke Lord LLP, was constantly helpful in her re-reading of many sections.

For the previous edition of this guide, Kirsten Whitfield, a Director with Gowling WLG in the U.K., along with Amelia Angus and Mike Reed, at the time both trainee solicitors at that firm, worked to organise, edit and otherwise facilitate the production of that earlier version – without which the current version would not have been possible.

Shelley Boyes, World Law Group Director of Marketing & Communications, kept us on track (a never easy task), and helped with final proofing and production of this guide.

The WLG is exceedingly grateful for the truly hard work, fine efforts and determination of all of these individuals and firms in helping us see this project through to conclusion.

II. ABOUT THE WORLD LAW GROUP

World Law Group is a network of 54 leading independent law firms with more than 350 offices in major commercial centres worldwide. WLG member firms comprise more than 18,000 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 & Data Protection Group

The World Law Group's Privacy & Data Protection 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. Many of them worked on this guide. The group's goal is to enhance the provision of relevant and seamless client services, including advising on cross-border data transfers, privacy risk assessments 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 and data protection issues and challenges for multinational and locally based clients, and 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 member firms and clients.

Members have also recently collaborated to produce an expanded 2016 edition of the WLG's respected *Global Guide to Whistleblowing Programs*, which will be available soon at www.theworldlawgroup.com.

1. ARGENTINA

1.1 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 Argentina law to notify either affected individuals or the Direccion Nacional de Proteccion de Datos Personales ("DPA") of a data breach.

However, according to Law No. 25,326 as amended (the Data Protection Law or "DPL") the data collector must adopt all technical and organisational measures necessary to ensure the security and confidentiality of the personal data, so as to avoid its alteration, loss, or unauthorised access or treatment. Such measures must permit the data collector to detect intentional and unintentional breaches of information, whether the risks arise from human action or technical means. In light of the foregoing, a certain implicit general obligation of notifying affected individuals of data breaches becomes applicable, at least to prevent or mitigate contingent liabilities arising from dissemination. The foregoing is consistent with the new provisions of the Civil and Commercial Code which have come into force recently.

In addition, storing personal data in files, registers or banks that do not meet technical integrity and security requirements is forbidden.

Note that the DPA, under its General Disposition No. 11/2006, has established three levels of security measures according to the nature of personal data being processed, providing different security measures to be adopted according to the level of security applicable to the data. Those security measures must be included in a mandatory data protection protocol, which shall contain all the security rules of the relevant company acting as data holder, in compliance with the provisions of the DPL and General Disposition No. 11/2006 (as amended by General Disposition No. 9/2008) of the DPA.

Notwithstanding the level of security applicable to each case, those protocols mentioned in the foregoing paragraph must contain certain rules creating a Registry of Security Incidents, incorporating a procedure for Notification, Management and Response in case of a data breach. According to Disposition 9/2008 of the DPA, at a minimum this procedure must include an internal notification procedure in order to keep a record of the incidents, but it does not require any kind of notification to the affected individuals or the DPA.

The DPA is entitled to inspect 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 Registry of Security Incidents), and to enforce the legal framework by applying penalties, which may be later revised at the courts of law.

1.2 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 case a breach of substantial information has occurred, and notifying the affected individual may help in preventing or mitigating damages to be suffered by the affected individual, the data holder (either a data controller or a data processor) shall have a certain implicit general obligation to notify the affected individual of the data breach. The foregoing is consistent with the new provisions of the Civil and Commercial Code of Argentina that have come into force recently.

1.3 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?

Content of the notice should identify the data that has been disseminated and the way in which it has been disseminated. Such a notice should be delivered as promptly as practicable to help in preventing or mitigating damages to the fullest possible extent. The method for serving such notice would be either: (1) any way in which an acknowledgement from the addressee can be obtained, or (2) through a formal letter with certificate of receipt (Carta Documento) sent through the Argentine Post Office (Correo Argentino).

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

The risks of failing to notify the affected individuals are incurred in civil liability for not having adopted reasonable actions to mitigate or prevent damage as a result of the breach. The foregoing is consistent with the new provisions of the Civil and Commercial Code of Argentina.

1.5 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 analysed on a case-by-case basis when deciding whether to notify an individual of a data breach. Key factors to be assessed 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. It should be considered that in light of the new Civil and Commercial Code, the liability of the data holder (either a data controller or a data processor) may increase if it does not adopt reasonable measures to prevent or mitigate the damage.

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

The main data protection national laws and regulations are:

- Section 43 of the Argentine Constitution and the DPL grant prompt court protection ("habeas data court remedy") to any type of information related to identified or identifiable individuals or legal entities ("Personal Data") contained in public and private databases. Affected individuals are entitled to demand amendment, updating, confidentiality, or suppression (if inaccurate) of such information;

- The DPL and its Regulatory Decree No. 1558/2001 also contain, among other provisions: general data protection principles, the rights of affected individuals, the obligations of data holders (either data controllers or data processors), 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 of Law No. 25,326, 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;

- Any public or private database formed for the purpose of providing reports, any private database that is not formed exclusively for personal use, and any database formed for the purpose of transferring personal data must be registered with the DPA, per the DPL and ancillary regulations;

- Criminal Code, Sections 117*bis* and 157*bis* address crimes regarding personal data violations such as knowingly inserting false information in a database, knowingly providing false information from a database, illegally accessing a restricted database, or revealing information contained in a database that the offender was in charge of keeping confidential. Criminal violations are subject to prison terms ranging from one month up to three years, which may be increased by 50% if any person suffers damage as a result of the crime.

In addition, there are a number of dispositions issued by the DPA, including:

- Disposition No. 2/2005, which created the National Registry of Databases and provides for the compulsory registration of certain databases with this 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.

1.7 Contact information for Data Protection Authority:

Name:	Dirección Nacional de Protección de Datos Personales
Address:	Sarmiento 1118 – 5º Piso; Ciudad Autónoma de Buenos Aires; Buenos Aires, Argentina (C1041AAX)
Telephone:	+54 11 4383 8512
Email:	infodnpdp@jus.gov.ar
Website:	www.jus.gov.ar/datos-personales.aspx

For more information, contact:

Name:	Carlos E. Alfaro
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
Website:	www.alfarolaw.com

2. AUSTRALIA

2.1 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 under Australian law to notify either affected individuals or the regulator, which is the Office of the Australian Information Commissioner ("OAIC"), of a data breach.

Mandatory data breach notification legislation has been on the Commonwealth Government agenda for some years and has been recommended by the Australian Law Reform Commission. Amendments to Commonwealth data protection laws that would have required organisations and Commonwealth government agencies to notify affected individuals and the OAIC of any "serious data breach" were before Parliament in 2013, but lapsed after Parliament was prorogued ahead of the Federal election. However, in response to a recommendation from a Parliamentary Joint Committee advising on national security reforms – that mandatory laws are introduced to help balance the increased risks associated with the Government's proposed mandatory data retention scheme – the Government has released for consultation an exposure draft Bill for mandatory notification of serious data breaches. The Government proposes to then finalise the Bill for introduction to Parliament. The Bill, which would amend the Commonwealth data protection laws and aims to introduce a scheme that protects individual privacy without placing an unreasonable regulatory burden on business, is similar to the 2013 proposal.

2.2 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.

2.3 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.

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

Not applicable.

2.5 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)?

Organisations are required by the Privacy Act 1988 to take reasonable steps to keep data secure. Notifying affected individuals may form part of those reasonable steps depending on all the circumstances of the breach. The OAIC's Data breach notification guide found here recommends that affected individuals and the OAIC should be notified if there is a risk of 'serious harm' occurring as a result of the breach. The Guide is not binding but is considered best practice and would support compliance with the reasonable steps obligations.

The proposed mandatory data breach legislation is likely to reflect the guidelines in a mandatory notification scheme.

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

The key legislation is the Commonwealth Privacy Act 1988.

2.7 Contact information for Data Protection Authority:

Name:	Office of the Australian Information Commissioner
Address:	GPO Box 5218, Sydney, NSW 2001, Australia
Telephone:	+61 2 9284 9749 (or if calling from Australia 1300 363 992)
Fax:	+61 2 9284 9666
Email:	enquiries@oaic.gov.au
Website:	www.oaic.gov.au

For more information, contact:

Name:	Veronica Scott
Firm:	MinterEllison
Address:	Rialto Towers, 525 Collins Street, Melbourne, VIC 3000, Australia
Telephone:	+61 3 8608 2126 or +61 3 8608 2654
Fax:	+61 3 8608 1181 or + 61 3 8608 1000
Email:	veronica.scott@minterellison.com
Website:	www.minterellison.com

3. AUSTRIA[1]

3.1 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 Data Protection Act 2000 ("DPA 2000"), the controller must immediately notify the data subject in an appropriate manner if the controller learns that data under its control has 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.

Specific data breach notification requirements apply to providers of public electronic communications services (telecommunications providers and internet service providers) according to Section 95a of the Austrian Telecommunications Act.

3.2 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.

3.3 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.

3.4 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.

3.5 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)?

Not applicable.

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

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

The DPA 2000.

3.7 Contact information for Data Protection Authority:

Name:	Österreichische Datenschutzbehörde
Address:	Hohenstaufengasse 3, 1010 Vienna, Austria
Telephone	+43 1 531 15 / 202525
Fax:	+43 1 531 15 / 202690
Email:	dsb@dsb.gv.at
Website:	www.dsb.gv.at

For more information, contact:

Name:	Robert Keisler or Dr. Bernt Elsner
Firm:	CMS Austria
Address:	Gauermanngasse 2, 1010 Vienna, 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

4. BELGIUM[2]

4.1 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 obligation in Belgium to provide notification of data breaches to the affected individuals or to the regulator with the following exception.

The Act on Electronic Communications of 13 June 2005 requires notification of 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 provide notification of data breaches to the Privacy Commission (i.e., the DPA) immediately upon the occurrence of each data breach. The Privacy Commission immediately informs the Belgian Institute for Postal Services and Telecommunications of the 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 affected by the breach (Art. 114/1 §3 of the Act). The Privacy Commission monitors compliance with this Act.

Moreover, the Belgian Data Protection Authority issued an opinion in which it recommends to notify any data breach to the DPA.

4.2 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 give notification in accordance with the response to Question 4.1 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-authorised 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).

4.3 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, notification to individuals must contain the following information:

- The nature of the personal data breach;

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

- The contact points for more information; and
- The measures that are recommended to mitigate the adverse effects of the data breach.

The notification to the Privacy Commission 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 resolve 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 email and regular mail are recommended.

4.4 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 there are no penalties. With regard to breaches covered by the Electronic Communications Act, this legislation does not provide for criminal penalties. But general administrative penalties may apply: the Belgian Institute for Postal Services and Telecommunications may impose a fine of up to 5% of the turnover of a telecoms operator in case of a breach of the telecom regulations, which includes a failure to notify the data breach (art. 21 of the Act of 17 January 2003).

4.5 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 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 limit damage.

4.6 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 response to Question 4.1, above.

4.7 Contact information for Data Protection Authority:

Name:	Commission for the Protection of Privacy
Address:	Rue de la Presse 35, 1000 Brussels, Belgium
Telephone:	+32 2 274 4800
Fax:	+32 2 274 4835
Email:	commission@privacycommission.be
Website:	www.privacycommission.be

For more information, contact:

Name:	Tom Heremans and Tom De Cordier
Firm:	CMS Belgium
Address:	Chaussee de La Hulpe 178, B-1170 Brussels, Belgium
Telephone:	+32 2 743 6973
Fax:	+32 2 743 6901
Email:	tom.heremans@cms-db.com / tom.decordier@cms-db.com
Website:	www.cms-db.com

5. BOSNIA AND HERZEGOVINA

5.1 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 ("BiH"), 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 is not obligated to) file a complaint to the Personal Data Protection Agency of the BiH.

5.2 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 has been breached, or that his/her data was not handled fairly, the individual has the right to object and to ask the DPA that:

- The controller or processor refrains from such actions and corrects the factual situation caused by these actions;
- The controller or processor corrects or amends personal information so that it is authentic and accurate; and/or
- 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.

5.3 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 note that the complainant wants to stay anonymous;
- The name of the controller or the data processor against whom the complaint has 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 DPA by mail, fax or email. Alternatively, the complaint may be made in person to the Agency or by telephone with written notice following. The complainant may declare a preference to remain anonymous, but the Agency shall inform him/her that in this case the complainant will not be advised on the measures undertaken to address his/her complaint.

5.4 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 EUR 5,000 up to EUR 50,000 may be imposed on the controller.

5.5 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 affected individuals of a data breach.

5.6 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).

5.7 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 72 6250
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
Website:	www.cms-rrh.com/Bosnia-Herzegovina

6. BRAZIL

6.1 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 affected individuals. As further explained in 6.6 below, currently, there is a draft of a Bill of Law dealing with data protection matters under discussion, which provides for the creation of a "competent body" responsible for data protection matters. It would, presumably, perform the role of a data protection authority. However, the scope and characteristics of this "competent body" are still unclear.

6.2 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.

6.3 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.

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

Not applicable.

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

6.6 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 law 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 Defense Code, the Criminal Code and the recently enacted Brazilian Internet Act (the so called

Marco Civil da Internet). These pieces of legislation deal with different elements 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.

As a preliminary clarification, it is important to highlight that there is no definition of "personal data" in Brazilian law. It is our understanding, however, based on decisions of the Brazilian courts, that any data that may be used to identify an individual should be considered personal data for the purposes of data privacy rules (and which would encompass, for instance, the name, identification number and taxpayer number of the data subject).

Data privacy regulation – general

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 damages 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 unauthorised disclosure or collection of personal information or any violation of privacy rights. In these lawsuits, individuals may seek material and/or non-material damages. Damages 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 to inform the individual or to rectify negative credit information held in databases).

The Consumer Defense Code deals with consumer-related databases, data collection, and penalties for infringement of the corresponding provisions. According to the Consumer Defense Code, the consumer's consent is mandatory for the collection of his/her personal data or, alternatively, the consumer must be informed, in writing, about any data collection. In a case where the consumer requests the inclusion of his/her information, no communication is necessary.

Note that although, in principle, an informed consent is sufficient to validate consumers' data collection, the consolidated understanding of Brazilian consumer protection authorities and courts is that *express* consumer consent must be obtained before the collection of personal data. Any sort of implied consent is not sufficient to legitimize the data collection.

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 five 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 to correct or update data must 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.

The Brazilian Internet Act, effective since 23 June 2014, establishes principles, guarantees, rights and duties relating to the use of the internet in Brazil. With regards to data collection, it (i) corroborated the general privacy principle of the Consumer Defense Code, in the sense that data subjects are entitled to have the collection, use, storage and treatment of personal data subject to his/her prior and express consent; and (ii) further determined that provisions regarding collection, use, storage and treatment of personal data must be highlighted in the applicable agreement/terms of use of internet applications.

Furthermore, the Brazilian Internet Act created data retention obligations to internet connection providers (those that promote the transmission of data packages among terminals over the internet, upon the assignment or authentication of an IP address, e.g., carriers) and application providers (those that provide a set of features that may be accessed by a terminal connected to the internet, e.g., websites).

Connection registrations (meaning information regarding the date and hour a connection begins and ends and the IP address used for sending and receiving data packages) must be stored by connection providers under secrecy for a one-year term.

Registrations of access to internet applications (meaning information regarding the date and hour the use of an application begins and ends from a given IP address), on the other hand, must be stored for a six-month term (subject to extension upon request from the police authorities, administrative authorities or the Ministry of Public Prosecution) by application providers that either (i) are organized as legal entities; and (ii) use applications as an instrument for the exercise of economic activities.

The Brazilian Internet Act also establishes that users may always request the deletion of their personal data from the database of internet applications, at the end of the relationship with the provider and such right will not be applicable only in the aforementioned hypothesis of mandatory retention.

There is a draft regulation of the Brazilian Internet Act submitted to public consultation between January and February, 2016, covering, among other things, security standards to be followed by connection and content providers when storing personal data, including:

- Strict control over access to personal data, including liability rules applicable to those who will be able to access personal data;
- Authentication mechanisms for access to registries, including, for instance, double authentication systems, in order to ensure the identification of the person responsible for the registries;

- The creation of a detailed inventory of access to registries, including the time, duration and identity of the employee or person responsible for the access; registry management solutions that use cryptography or equivalent protection technologies in order to ensure data integrity; and

- A logical separation between registries and other data processing systems for commercial purposes.

For the purposes of the draft regulation, personal data is deemed any data related to an identified or identifiable individual, including identifying numbers, location data or electronic identifiers, (including connection and access registrations) as well as the content of private communications.

Notification requirements and international transfers of data

As a general rule, Brazilian law does not require any registration or notification to competent authorities prior to collecting or processing data. An exception to this general rule is established by the Consumer Defense Code and the Brazilian Internet Act. If the data at issue refers to consumers or is collected on the internet, consent is mandatory for the lawful collection of data. Nevertheless, we recommend that consent is obtained even for data collection of non-consumers outside the internet environment, to the extent any unauthorised data collection may be considered a breach of the constitutional right to privacy that, as explained above, applies to all Brazilians.

In this context, if a party intends to collect data it is advisable to write a privacy notice explaining the data collection in any form, which will be presented to data subjects 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 consent.

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 the 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 should 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 a transfer, either at the moment of collection or at the moment of the actual transfer.

With regard to international data transfer over the internet, it is worth noting that the Brazilian Internet Act establishes that, if personal data is collected in Brazil, the storage and treatment thereof shall occur in accordance with Brazilian law. Therefore, although there is no restriction for international transfer, Brazilian law must be complied with when the data is transferred and the consent of the data subject should be requested before the transfer.

The breach of the above may subject the infringer to penalties ranging from warning to fines in the amount of 10% of the net revenues of the infringer's economic group in Brazil and the suspension/prohibition of activities involving the collection, storage and treatment of personal data.

The procedure for the application of such penalties is still pending regulation, which will occur upon a Presidential Decree. Up to this moment, we do not have a forecast on when the Decree will be enacted and the approach that will be adopted in the regulation is still uncertain.

Prospective Brazilian data privacy legislation

Finally, the text of a Bill dealing with data protection in general was submitted for public consultation in January 2015. The consultation was completed in July 2015 and, following that, a new version of the Bill was prepared and released in October 2015, based on the consultations.

The first draft of the Bill mentioned in many of its provisions a "competent authority" which, presumably, would be a Brazilian data protection authority. The scope and characteristics of this "competent authority" were not clearly defined in the Bill; this was one of the points of discussion for the public consultation.

The first draft of the Bill also proposed a legal concept of personal data, describing it as "any information related to an identified or identifiable individual, including numbering identification, location data and electronic identifiers, including 'sensitive data'".

As per the Bill, "sensitive data" correspond to personal data that reveals racial or ethnic origins, religious, philosophical or moral convictions, affiliation to unions or organisations of a religious, philosophical or political character, data relating to health or sexual life, as well as genetic data.

With regard to data collection, the Bill also provided that the collection of private data shall depend on the express and specific consent of the individual whose data is being collected and that he/she shall be informed, at the moment of the collection, the purpose for which his/her private data will be used.

Specifically, with regard to the collection and transfer of personal data in the context of the rendering of a telecommunication service, note that Section 72 of Law No. 9,472/1997

(the "Brazilian Telecommunications Law") expressly states that the transfer of aggregated consumers' data, which do not directly or indirectly identify them or violate their privacy, does not require any consent.

The above-mentioned Bill also introduces innovations regarding international transfer of data. Cross-border transfers of personal data would be allowed only to countries granting a level of protection of personal data equivalent to that of Brazil, except when the transfer is expressly and specifically consented to by the data subject or is (i) necessary for cooperation among international public investigation bodies, as provided in treaties to which Brazil is a party; (ii) necessary to protect the life or physical integrity of the data subject or a third party; (iii) authorised by the "competent body"; (iv) resulting from obligations assumed in international cooperation treaties; (v) necessary for the execution of public policies or legal attributions of the public services. The evaluation of the level of protection of countries and the determination of security standards to be followed in Brazil will be incumbent upon the "competent body".

6.7 Contact information for Data Protection Authority:

Not applicable.

For more information, contact:

Name:	Marcela Waksman Ejnisman or Felipe Borges Lacerda Loiola
Firm:	TozziniFreireAdvogados
Address:	Rua Borges Lagoa, 1328, Sao Paulo, SP, 04038-904, Brazil
Telephone:	+55 11 5086 5000
Fax:	+ 55 11 5086 5555
Email:	mejnisman@tozzinifreire.com.br or fblacerda@tozzinifreire.com.br
Website:	www.tozzinifreire.com.br

7. BULGARIA[3]

7.1 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 Bulgarian legislation, in case of an established data breach there is no legal obligation to inform the Bulgarian regulator ("Commission for Personal Data Protection"), or the affected individuals.

Specific data breach notification requirements apply to providers of electronic communication services (telecommunications providers and internet service providers). In December 2011, the provisions of 2009/236 of the European Parliament and of the Council regarding breaches of personal data were implemented in the Bulgarian Electronic Communications Act.

In conformity with the requirements of that regulation, Bulgarian law envisages that in the case of a breach of personal data, the provider of electronic communication services shall notify the Commission for Personal Data Protection within three days after detection of the breach. Where such a breach is likely to adversely affect the personal data or privacy of a subscriber or another person, the provider of electronic communication services shall also notify, in due time, the subscriber or the person that is the subject of the data breach.

7.2 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 except in the cases connected with the provision of electronic communication services, as described in the response to Question 7.1 above.

7.3 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 except in the cases connected with the provision of electronic communication services, as described in the response to Question 7.1 above. There is no specific guidance on the content or method of giving notice but, in general, communication with the Bulgarian Commission for Personal Data Protection is in written form (applications, letters, notifications etc.).

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

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

Any provider of public electronic communication services that fails to comply with the obligations referred to in the response to Question 7.1 above, shall be liable for a penalty ranging from BGN 2,000 (approx. EUR 1,000) up to BGN 20,000 (approx. EUR 10,000). In case of repeated violations of said obligations, a penalty up to an amount double the amount of the initial penalty may be imposed (up to BGN 40,000).

7.5 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.

7.6 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;
- Rules on the activity and the administration of the Commission for Personal Data Protection;
- Ordinance No 1 dated 30 January 2013, on the minimum level of technical and organisational measures and the admissible type of personal data protection;
- Electronic Communications Act;
- Civil Registration Act.

7.7 Contact information for Data Protection Authority:

Name:	Commission for Personal Data Protection
Address:	2 Prof. Tsvetan Lazarov Blvd., 1592 Sofia, Bulgaria
Telephone:	+359 2 9153 518
Email:	kzld@cpdp.bg
Website:	www.cpdp.bg

For more information, contact:

Name:	Marin Drinov
Firm:	CMS Bulgaria
Address:	4 Knyaz Alexander I Battenberg Str., fl. 2, 1000 Sofia, Bulgaria
Telephone:	+359 2 447 1317
Fax:	+359 2 447 1390
Email:	marin.drinov@cms-rrh.com
Website:	www.cms-rrh.com

8. CANADA

8.1 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)?

Federal

At the federal level, the Personal Information Protection and Electronic Documents Act SC 2000, c. 5 ("PIPEDA") has been enacted and is designed to protect the collection, disclosure or use of personal information. PIPEDA was recently amended by the Digital Privacy Act (through Bill S-4) to include, among other things, notification obligations for organisations in the event of a breach of security safeguards involving personal information under an organisation's control. The amendments also create an obligation to report such breaches to the Privacy Commissioner. The breach notification requirements are not yet in force as of this writing.

Provincial

Canada is a federal State composed of 10 provinces. At the provincial level, there is no requirement to notify the affected individuals or a data protection authority[4], with the exception of:

- In 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
- In the province of Nova Scotia with respect to health-related personal information.
- The province of Manitoba has passed a new statute, The *Personal Information Protection and Identity Theft Prevention Act*, S.M. 2013, c. 17 ("PIPITPA"), that includes a requirement to notify affected individuals. As of the date of this publication, PIPITPA is not yet in force.

[4] Please note that we have not considered laws that apply only to public sector entities.

8.2 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?

Federal

Once in force, the PIPEDA amendments referred to in the response to 8.1 above will provide that any private-sector organisation that collects, uses or discloses the personal information of an identifiable individual in the course of commercial activities must notify an individual where there is a loss of, unauthorised access to, or unauthorised disclosure of personal information of the individual under the control of the organisation resulting from a breach of an organisation's security safeguards, and it is reasonable to believe that the breach creates a real risk of significant harm to the individual. In the above circumstances, the organisation is also required to report such breaches to the Privacy Commissioner.

Once the amendments are in force, an organisation will also be required to notify any other organisation or government entity of a breach if the notifying organisation believes that the other organisation or government entity will be able to reduce or mitigate the risk of the harm in question.

Significant harm includes bodily harm, humiliation, damage to reputation or relationships, loss of employment, business or professional opportunities, financial loss, identity theft, negative effects on credit records and damage to or loss of property. The factors that are relevant to determining whether a breach of security safeguards creates a real risk of significant harm to an individual include:

- The sensitivity of the personal information involved in the breach;
- The probability that the personal information has been, is being or will be misused; and
- Any other factor as may be prescribed by regulation.

Provincial

Half of Canada's provinces require breach notification in some circumstances, with four provinces confining such notification to health-related personal information. Only Alberta currently has a private-sector wide privacy breach notification requirement. Once PIPITPA is in force, Manitoba will also have a data breach notification requirement that will apply across the private sector.

Alberta

In Alberta, organisations that collect, use and disclose personal information about individuals must notify the Alberta Commissioner where there are losses of or instances of unauthorised 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 as a result of the loss or unauthorised access or disclosure.

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. 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.

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. 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 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.

Manitoba

Once PIPITPA is in force, organisations that have personal information in their custody or control will have to notify affected individuals if their personal information is lost, stolen, or accessed in an unauthorised manner, subject to certain exceptions, including where the organisation has satisfied itself that it is not a reasonable possibility that the information that has been lost, stolen, or accessed will be used unlawfully.

Ontario – Health Context Only

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 utilised, 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 unauthorised persons.

The obligation to notify generally applies to:

- Health information custodians;
- People that health information custodians disclosed personal health information to; or
- People who collect or use health numbers, or who have had health numbers disclosed to them.

Newfoundland and Labrador – Health Context Only

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 must inform the Privacy Commissioner of the breach. "Custodians" are certain classes of people 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. A custodian must also notify the individual who is the subject of the information where such information is stolen, lost, disposed of in an unauthorised manner, or disclosed or accessed by an unauthorised person, unless the custodian does not believe that the theft, loss, unauthorised disposition or improper disclosure or access of personal information will have an adverse impact on the provision of health care or benefits to the individual, or on the well-being of the individual to whom the information relates.

New Brunswick – Health Context Only

A custodian must notify the individual to whom the information relates and the provincial privacy commissioner at the first reasonable opportunity if personal health information is stolen, lost, disposed of (except as permitted by relevant legislation), or disclosed to or accessed by an unauthorised person, unless the custodian reasonably believes that the theft, loss, disposition, disclosure or access will not:

- Have an adverse effect on the provision of health care or benefits to the individual to whom the information relates;
- Have an adverse impact on the well-being of the individual to whom the information relates; or
- Could 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 – Health Context Only

A custodian that has custody or control of personal health information about an individual must notify an individual if the health professional reasonably believes that:

- Their information is stolen, lost or subject to unauthorised access, use, disclosure, copying or modification; and
- 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 must notify the provincial privacy review officer as soon as possible.

8.3 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?

Federal

Once the amendments to PIPEDA are in force, a notification provided to an individual by an organisation must provide sufficient information to allow the individual to understand the significance to him/her of the breach and to take steps, if any are possible, to reduce the risk of harm or mitigate the harm that could result from the breach. The notification must be conspicuous and given directly to the individual.

Where an organisation is required to notify an individual or organisation, or report to the Privacy Commissioner, in respect of a breach of security safeguards, the organisation is required to give such notification or make such report as soon as feasible after the breach has occurred.

Provincial

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;
- A description of the personal information involved in the breach;
- An assessment of 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;
- A description of any steps the organisation has taken to reduce the risk of harm;
- A description of any steps the organisation has taken to notify individuals; and
- Contact information for a person who can answer, on behalf of the organisation, the Alberta Commissioner's 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 date on which or the time period during which the breach occurred;
- A description of the personal information involved;
- A description of any steps the organisation has taken to reduce the risk of harm; and
- Contact information for a person who can answer, on behalf of the organisation, questions about the breach.

Notice to the Alberta Commissioner 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.

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, in which case indirect notification is acceptable.

Manitoba

Once PIPITPA is in force, notice will have to be given as soon as it is reasonably practicable for an organisation to do so. Currently, no method of notification has been specified, nor is there any required or suggested content.

Ontario, Newfoundland and Labrador, New Brunswick and Nova Scotia – Health Context Only

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.

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

Federal

Upon the enactment of Bill S-4, an organisation that fails to: (i) report a breach of security safeguards involving personal information under its control to the Privacy Commissioner; or (ii) notify an individual of a breach of security safeguards involving the individual's personal information under its control; is guilty of an offence punishable on summary conviction and liable to a fine not exceeding CAD 10,000, or an indictable offence and liable to a fine not exceeding CAD 100,000.

Provincial

Alberta

PIPA provides for a fine of no more than CAD 100,000 for organisations and CAD 10,000 for individuals who fail to notify the Alberta Privacy Commissioner when required to.

Manitoba

PIPITPA provides that it is an offence, among other things, to willfully collect, use or disclose personal information in contravention of certain provisions of PIPITPA, or to willfully attempt to gain or gain access to personal information in contravention of PIPITPA. These offences, amongst others, are punishable by a fine of no more than CAD 100,000 for organisations or CAD 10,000 for individuals. PIPITPA also provides that an individual may commence an action against an organisation for failing to provide notice of a data breach when required to do so.

Ontario

Willful disclosure or use of personal health information in contravention of the legislation is an offence, as is willfully 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 CAD 250,000 for organisations and CAD 50,000 for natural persons.

Newfoundland and Labrador

Willful disclosure or use of personal health information in contravention of the legislation is an offence, as is willfully obstructing the Newfoundland and Labrador Privacy Commissioner in the performance of his or her duties under the legislation. These offences, amongst others, are punishable by a fine of not more than CAD 10,000 or imprisonment for a term not exceeding six months, or both.

New Brunswick

Disclosure or use of personal health information in willful contravention of the legislation is an offence, as is obstructing the New Brunswick Privacy Commissioner in the performance of his or her duties under the legislation. These offences, amongst others, are punishable by a fine of between CAD 240 and CAD 10,200 for a first offence.

Nova Scotia

Willful disclosure or use of personal health information in contravention of the legislation is an offence, as is willfully obstructing, making a false statement to, or misleading or attempting to mislead the provincial review officer. These offences, amongst others, are punishable, in the case of a corporation, by a fine of not more than CAD 50,000 and in the case of an individual, by a fine of not more than CAD 10,000 or imprisonment for six months or both.

8.5 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 privacy regulator and only until the amendments provided for by Bill S-4 come into force.

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 minimize 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 also provide 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.

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 version of the Guidelines and summary checklist are available at:

www.priv.gc.ca/information/guide/2007/gl_070801_02_e.asp;

www.priv.gc.ca/information/guide/2007/gl_070801_checklist_e.asp.

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

- Canada (Federal): Personal Information Protection and Electronic Documents Act, SC 2000, c 5.
- Alberta: Personal Information Protection Act, S.A. 2003, c. P-6.5.
- Manitoba: The Personal Information Protection and Identity Theft Prevention Act, S.M. 2013, c. 17.
- 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.

8.7 Contact information for Data Protection Authority:

Federal

Name: Office of the Privacy Commissioner of Canada
Address: 30 Victoria Street, Gatineau, Quebec, K1A 1H3, Canada
Telephone: +1 819 994 5444 or +1 800 282 1376
Fax: +1 819 994 5424
Email: via online request form: www.priv.gc.ca/cu-cn/index_e.asp
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: +1 403 297 2711
Email: generalinfo@oipc.ab.ca
Website: www.oipc.ab.ca

Manitoba

Name: Manitoba Ombudsman
Address: 750-500 Portage Avenue (Colony Square), Winnipeg, MB, R3C 3X1
Telephone: +1 204 982 9130 or +1 800 665 0531
Fax: +1 204 942 7803
Email: ombudsman@ombudsman.mb.ca
Website: www.ombudsman.mb.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:	Peter Ruby or Rachel Ouellette
Firm:	Goodmans LLP
Address:	Bay Adelaide Centre, 333 Bay Street, Suite 3400 Toronto, Ontario, Canada, M5H 2S7
Telephone:	+1 416 979 2211
Fax:	+1 416 979 1234
Email:	pruby@goodmans.ca or rouellette@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

9. CHILE

9.1 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 the event 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.

9.2 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.

9.3 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.

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

Not applicable.

9.5 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 information database must pay economic and/or immaterial damages in case of improper treatment, or eliminate, modify or block the corresponding data, upon request of the owner or if ordered by a court.

9.6 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 may only be used when authorised by law or when the owner of the data gives 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 that 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, sexual 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 the owner.

There are some exceptions to the obligation to obtain an authorisation 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 insofar 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 authorisation from the owner of personal data is required in certain cases, such as the handling of personal data that comes or is collected from public sources and that has a financial, banking 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 for a public or governmental job.

9.7 Contact information for Data Protection Authority:

Not applicable.

For more information, contact:

Name:	Sergio Orrego Flory
Firm:	Urenda Rencoret Orrego y Dörr
Address:	Avenida Andres Bello No 2711, Piso 16, Las Condes, Santiago de Chile, Santiago, Chile, 7550611
Telephone:	+56 2 2499 5500 or +56 2 499 5507
Fax:	+56 2 2499 5555
Email:	sorrego@urod.cl
Website:	www.urod.cl

10. CHINA

10.1 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 data protection law in China although the Personal Information Protection Law was drafted in 2008. However, the revised Consumer Rights Protection Law, which took effect on 15 March 2014, requires that: "In the event of disclosure or loss or possible disclosure or loss of personal information, remedial measures shall be forthwith adopted by business operator(s)".

Based on our communications with law enforcement authorities, notification to individuals in the event of a data breach affecting residents will be a necessary remedial measure.

There is no specific data protection agency ("DPA") in China either. According to various regulations stipulated by different government agencies, business operators shall report certain data breaches to the competent government agencies. For example, the local People's Bank of China ("PBOC") in the banking and finance sector, and the telecommunications administration in the telecommunications and internet services industry.

10.2 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 February 2009, "personal information" was introduced in Amendment VII to the Chinese Criminal Law. Since then, "personal information" instead of "personal data" has been referred to in various laws and regulations.

For example, on 16 July 2013, the Ministry of Industry and Information Technology ("MIIT") stipulated Provisions on Protecting the Personal Information of Telecommunications and Internet Users ("MIIT Provisions"). MIIT defines "personal information of users" as the information collected by telecommunication business operators and internet information service providers during the provision of services that may be used for identifying the users and the timing, places, etc., of the use of services by the users either independently or in combination with other information, and shall include the name, date of birth, identity document number, address, phone number, account number, password, etc., of a user.

On 5 January 2015, the State Administration for Industry and Commerce ("SAIC") stipulated Measures for Punishments against Infringements on Consumer Rights and Interests ("SAIC Measures"), which is an implementation rule of China's Consumer Rights Protection Law. According to the SAIC Measures, consumers' personal information shall refer to the information collected by a business operator during the provision of goods or services that may be used for identifying consumers either independently or in combination with other information, such

as the name, gender, occupation, date of birth, identity document number, residential address, contact details, income and asset conditions, health conditions and consumption habits of a consumer.

In China, there is no definition of "data controller" or "data processor." "Business operator" is referred to in the China Consumer Rights Protection Law, while "telecommunication business operator" and "internet information service provider" are referred to in the MIIT Provisions. In our view, "business operator" includes both data controllers and data processors.

10.3 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?

Currently, there is no law or regulation in China to provide any requirements regarding the content of the notice, or the method of giving notice.

As to the timing of providing notice, China's Consumer Rights Protection Law requires remedial measures to be forthwith adopted in the event of disclosure or loss (or possible disclosure or loss) of (personal) information.

As per a Circular of the People's Bank of China on Personal Financial Information Protection by Banking Financial Institutions ("PBOC Circular") which became effective on 1 May 2011, banking financial institutions ("BFI") shall give notice on the date when the disclosure 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 disposition opinion.

In June 2015, the 15th session of the Standing Committee of the 12th National People's Congress ("NPC") preliminarily reviewed the Network Security Law (Draft), which is promulgated at the website of the NPC for soliciting public comments. According to this draft, when the information is or might be divulged, damaged or lost, network operators shall take remedial measures immediately, notify the users who might be affected thereof and report the same to relevant competent authorities in accordance with relevant provisions.

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

China's Consumer Rights Protection Law stipulates that non-compliance may be subject to a warning and/or confiscation of illegal income, a fine ranging from one to 10 times the amount of illegal income based on the circumstances, or where there is no illegal income, a fine of not more than RMB 500,000 shall be imposed. In serious cases, the business operator shall be ordered to suspend business operation for correction and its business licence shall be revoked.

According to the MIIT Provisions, in case of non-compliance, telecommunications business operators and internet information service providers are subject to penalties including: being ordered to make correction within the prescribed time limit, warnings by telecommunications authorities, and a fine of not less than RMB 10,000 but not more than RMB 30,000. Their violations and punishments will also be announced to the public.

The draft Network Security Law stipulates that in case of non-compliance, the respective competent authority shall order the network operator to undertake correction and depending on the circumstances, issue a warning, confiscate its illegal gains or impose a fine of not less than the amount of the illegal gains but not more than 10 times that amount separately or concurrently. If there are no illegal gains, a fine of not more than RMB 500,000 shall be imposed. In case of serious breaches, the competent authority may order the network operator to suspend the relevant business activities or close the website. The authority may even revoke business permits or business licences and may impose a fine of not less than RMB 10,000 but not more than RMB 100,000 per person on those directly responsible as well as on other persons who are directly liable.

10.5 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 mentioned above, the revised China Consumer Rights Protection Law requires business operators to take remedial measures forthwith in case of a data breach, and we are of the opinion that notification to individuals in the event of a data breach affecting residents will be a necessary remedial measure.

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

As explained above, currently there is no comprehensive or general data protection law applicable in China, but a number of general laws have incorporated certain provisions relating to personal privacy protection to illustrate the principle of data protection. These include but are 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;
- China Consumer Rights Protection Law;
- Measures for Punishments against Infringements on Consumer Rights and Interests, effective 15 March 2015.

In addition, some laws, regulations or circulars regarding specific industry sectors also contain provisions on personal information/data protection, including but not limited to:

- Electronic Signature Law of the PRC, effective 24 April 2015;
- Rules Regarding the Protection of Personal information of Telecommunications and Internet Users Circular by the China Ministry of Industry and Information Technology ("MIIT") effective on 1 September 2013;
- The Regulations on Credit Reporting Industry effective on 15 March 2013;
- The Social Insurance Law of the PRC effective on 1 July 2011;
- Measures for the Supervision and Administration of Credit Card Business of Commercial Banks effective on 13 January 2011;
- The Statistics Law of the PRC effective on 1 January 2010;
- The Passport Law of the PRC effective 1 January 2007;
- The Interim Measures on Management of Personal Credit Information Basic Database effective on 1 October 2005; and
- The Resident Identity Cards Law of the PRC effective on 1 January 2004.

Overall, there are about 40 laws, 30 regulations and more than 200 provisions addressing personal information protection, whether directly or indirectly.

Information Security Technology Guideline

There is also 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 288282012, or the "Guideline"), which became effective on 1 February 2013. This is only a recommended standard and has no compulsory legal effect.

10.7 Contact information for Data Protection Authority:

In China, the authority in charge of data protection 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.

Other than MIIT, the State Internet Information Office is in charge of the cases of internet management, the Public Security Bureau (police) is in charge of criminal cases regarding data violation and breach, PBOC is in charge of data protection in the banking and finance sector.

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

In the event of a data breach, we suggest business operators contact the local competent authority directly.

For more information, contact:

Name:	Michael Shu
Firm:	Zhong Lun Law Firm
Address:	10-11/F, Two IFC, 8 Century Avenue, Pudong New Area, Shanghai 200120, People's Republic of China
Telephone:	+86 21 6061 3650
Fax:	+86 21 6061 3555
Email:	michaelshu@zhonglun.com
Website:	www.zhonglun.com

11. COLOMBIA

11.1 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.

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

Pursuant to Art. 3 of Law 1581 of 2012, the parties involved in the treatment of data in Colombia are defined as: (i) the data controller, any 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, any 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.

11.2 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 regarding the 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.

11.3 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.

11.4 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, Art. 23 determines that the DPA can impose the following fines and penalties on the data controller and the data processor:

- Fines up to USD 2 million;
- Suspension of the activities related to data collection for up to six months;

- Temporary closure of operations related to data collection and data treatment; and/or
- Immediate and definitive closing of any operation that involves the processing of sensitive data.

11.5 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 notifications to individuals in the event of a data breach.

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

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

- Art. 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 1273 (2009), modifying the Criminal Code, pursuant to which illegitimate acquisition, promotion, exchange or other misuse of personal data constitutes a criminal offense;
- Statutory Law 1581 (2012), which sets out the legislation on personal data protection;
- Decree 1377 (2013), implementing regulation of Law 1581 (2012);
- Decree 886 (2014), which implements the National Registry of Databases; and
- External Circular Letter 02 (2015), which implements registration of personal databases on the National Registry of Databases.

11.7 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 competence 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:	German Enrique Bacca Medina (Deputy Superintendent for Personal Data Protection)
Address:	Bogotá, D.C., Colombia, Carrera 13, 27-00
Telephone:	+571 5870 247/227
Fax:	+571 5870 284
E-mail:	habeasdata@sic.gov.co

Superintendence of Finance:

Name:	Jorge Castaño Gutiérrez (Superintendent of Finance)
Address:	Calle 7 No. 4-49
Telephone:	+571 5940200/ 5940201 Ext. 1501 – 1502
E-mail:	jocastano@superfinanciera.gov.co
Website:	www.superfinanciera.gov.co/jsp/index.jsf

For more information, contact:

Name:	Diego Cardona
Firm:	Philippi, Prietocarrizosa, Ferrero DU & Uría
Address:	Carrera 9 # 74-08, Bogota D.C., Colombia,
Telephone:	+571 326 8600 Ext. 1419
Fax:	+571 326 8419
Email:	diego.cardona@ppulegal.com
Website:	www.ppulegal.com

12. COSTA RICA

12.1 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)?

According to Art. 38 of the regulation for the Data Protection Law (Executive Decree Nº 37554-JP published 5 March 2013), the responsible party (i.e., a position similar to the concept of a data controller under European law) of the database needs to inform the data owner about any irregularities in the treatment and storage of data, such as loss, destruction, or any similar data breach due to a security vulnerability.

If the responsible party becomes aware of a data breach, the responsible party will have five working days following the data breach to report the breach, so that the holders of such personal data may take appropriate actions.

Within the same time, the responsible party must initiate a comprehensive review to determine the extent of the issue, and corrective and preventive actions need to be taken, as appropriate.

According to Article 39 of the regulation for the Data Protection Law, the responsible party of the database must inform the holder of such personal data and the Data Protection Authority ("PRODHAB"), of any security vulnerabilities that have arisen. The notification must include at least the following:

- The nature of the incident;
- Personal data that was subject to the data breach incident;
- Corrective actions taken; and
- The means or the place where appropriate/authorised personnel can get more information.

The responsible party must keep a register of security incidents. In addition, the law requires that security measures must be established if a data breach incident occurs.

The law makes a distinction between a party responsible for a database (i.e., the "responsible party") and a party handling a database ("handling party"), which is illustrated by the definitions in the law provided below.

"The party responsible for the database is a physical or legal person *that administers, manages or is in charge of the database*, whether this is a public or private entity, which is competent under the law *to decide the purpose of the database, what categories of personal information will be registered in it and what type of treatment will be applied to it*."[5] (Emphasis not in original).

[5] Article 3 of the *Law on Individual Protection for Processing of Personal Data.*

"Party Handling Databases: All physical and legal persons, whether public or private, or any other entity *that handles personal data for the account of the party responsible for the database.*"[6] (Emphasis not in original).

PRODHAB takes the position that if an entity both undertakes the part of the responsible party and the handling party at the same time, PRODHAB should be informed of this.

The responsible party and the handling party must sign an acceptance letter in which the handling party accepts its position and which lays out the specific obligations assumed by the handling party. This letter must be signed and presented to PRODHAB in the registration application.

The responsible party will determine the security measures applicable to the personal data handled or stored, considering the following factors:

- The sensitivity of the personal data handled, as permitted by law;
- The state of technology development;
- The possible consequences of a breach for the owners of the personal data;
- The number of owners of personal data;
- The breaches that have previously occurred in the handling and storage systems being used;
- The risk presented to the personal data based on their quantitative or qualitative value; and
- Other factors that arise under other laws or regulations applicable to the responsible party.

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 party responsible for the database must inform the data owner and PRODHAB, about any irregularities in the treatment and storage of data, such as loss, destruction, or any similar data breach due to a security vulnerability.

If the data breach affects the data holder, he/she can file an administrative claim before PRODHAB. PRODHAB may run an investigation, and the company may face fines if the database is not recorded or their security measures have been violated.

[6] Article 2 of the Regulation to the *Law on Individual Protection for Processing of Personal Data.*

In Costa Rica, the misuse or violation of personal data has been defined as a crime. In accordance with Art. 196 bis of the Costa Rican Criminal Code, a three- to six-year prison term may be imposed on the legal representative of the company if the company accesses, seizes, modifies, interferes, copies, transmits, publishes, disseminates, compiles, disables, intercepts, retains, sells, buys, diverts for a purpose other than for which they were collected, or uses the images or information it has stored, without consent.

On the other hand, the Data Protection Law establishes two types of faults classified as "minor" and "serious".

- Minor faults include:

(a) Collecting personal data without explaining to the owner of the information why the data is being collected; and

(b) Collection, storage and transfer to third parties, of personal data by unsecure means.[7]

A fine up to five minimum salaries will be imposed if any of the above is committed. In Costa Rica, "minimum salaries" means minimum wage and it is a way of quantifying a fine. The basic wage in Costa Rica Colónes (CRC) is CRC 424,200 (around USD 780), so this fine could be up to approximately USD 3,900.

- Serious faults include two categories: minor serious faults and major serious faults.

- Minor serious faults:

(a) Collection, storage and transfer by any means as well as use of personal data without informed and express consent of the owner of the data;

(b) Transfer of personal data to third parties without complying with the law;

(c) Collection, storage, transfer or use of the personal data for a purpose other than that authorised by the owner of the information;

(d) Denial to the owner of the personal information access to his/her personal data stored by the company in its databases; and

(e) Denial of deleting or rectifying personal data.[8]

A fine of five to 20 minimum salaries (USD 3,900 to 15,600) will be imposed if any of the above is committed.

- Major serious faults:

(a) Collecting, storing, transferring or using by any means of sensitive data without complying with the Data Protection Law;

[7] Article 29 of Data Protection Law.
[8] Article 30 of Data Protection Law.

(b) Obtaining personal data from the owner of the data or third parties, in a manner which involves violence, threat or deception;

(c) Revealing registered information from a database that is required to remain undisclosed;

(d) Transferring to a third party information that has been changed to different or false information from that originally provided by the owner of the data;

(e) Implementing and using a database that has not been registered with PRODHAB; and

(f) Transferring the database or parts of the database to a third party in a foreign country without prior consent.[9]

A fine of 15 to 30 minimum salaries (from about USD 11,700 to 23,400) will be imposed if any of the above is committed and a suspension of one to six months.

If any of these faults arises, the data holder may request an administrative and/or judicial investigation.

12.3 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?

To notify PRODHAB of a data breach, the notification must include at least the following:

- The nature of the incident;
- Personal data that was subject to the data breach incident;
- Corrective actions taken; and
- The means by which or where appropriate/authorised personnel can get more information.

Note that this notification applies to databases that are registered with PRODHAB. If a database includes sensitive or restricted information, if it will be transferred outside the country, or if its contents will be sold, distributed or shared with a third party, then the database should be registered with PRODHAB.

Once all the forms and functional requirements are fulfilled by the applicant, an annual fee of USD 200 must be paid to PRODHAB to finalize the registration of the database.

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

See the penalties and fines listed in the response to Question 12.2 above.

[9] Article 31 of Data Protection Law.

12.5 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 every data breach must be provided to the individual and to PRODHAB if it is due to a security vulnerability.

It is recommended to conduct due diligence on the databases subject to notification procedures and register them with PRODHAB.

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

The main data protection national laws and regulations are:

- Case law of the Constitutional Court;
- Law for the protection of the individual regarding the treatment of their personal data, Nº 8968 dated 7 July 2011;
- Executive Decree Nº 37554-JP published 5 March 2013, on page 42 of the Official Daily Newspaper *La Gaceta* Nº 45, containing the Regulations to the Law for the protection of the individual regarding the treatment of their personal data; and
- Article 196 bis of the Costa Rican Criminal Code.

12.7 Contact information for Data Protection Authority:

Name:	Agencia de protección de datos de los habitantes (PRODHAB)
Address:	Edificio Administrativo del Registro Nacional (Módulo 8) 4° piso
Telephone:	+506 2234 7959
Email:	protecciondedatos@mj.go.cr
Website:	www.prodhab.go.cr

For more information, contact:

Name:	Valeria Aguero
Firm:	Arias & Muñoz
Address:	Costa Rica, Centro Empresarial Forum 1, Edificio C, oficina 1C1.
Telephone:	+506 2503 9873
Fax:	+506 2204 7580
Email:	vaguero@ariaslaw.co.cr
Website:	www.ariaslaw.com

13. CROATIA[10]

13.1 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 does not oblige the data controller or any other party to inform either the affected individual or the data protection authority if any (personal) data breach is detected.

If, however, the data breach constitutes a criminal offence under the Croatian Criminal Code, and if such a breach is detected by a public authority, the public authority is obliged to file a criminal complaint with the prosecution authorities.

If the data breach occurs in connection with a publicly available electronic communications service, the provider of the public electronic communications service must inform the Croatian Regulatory Agency for Networks Activities and the Croatian Data Protection Agency of such breach and, if the breach may harm the privacy of an individual, also the respective individual. The Electronic Communications Act, however, provides exceptions to this rule.

13.2 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 of a breach is mandatory only if the breach is committed while using a publicly available electronic communication service. The breach must involve any type of personal data. The notifying entity is the operator of the public electronic communication service. The notification of the Croatian Regulatory Agency for Networks Activities and the Croatian Data Protection Agency is obligatory irrespective of the nature of the breach. The affected individual must only be informed if the breach is likely to harm his/her personal data or privacy. If, however, the operator proves to the Croatian Regulatory Agency for Networks Activities that adequate technical security measures were adopted for the respective data, the described notification to the affected individual is not required. However, the Croatian Data Protection Agency can request the operator of a publicly available electronic communications service to inform the affected individual if the breach could cause harm to the affected individual or another individual.

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

13.3 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 has mandatory content only in case of a breach through a publicly available electronic communications service. In such case, the notification to the affected individual must include the description of the data breach, contact data for further information and the suggested measures to mitigate potentially harmful consequences of the data breach. The notification to the Croatian Regulatory Agency for Networks Activities must also contain a description of the consequences of the data breach and the suggested or undertaken measures due to the breach.

The notification to the Croatian Regulatory Agency for Networks Activities and the notification to the affected individual should be made with no delay.

The method and form of the notice are not stipulated.

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

Failure to report a breach committed while using a publicly available electronic communication service may result in a fine from HRK 100,000 (approx. EUR 13,500) to HRK 1,000,000 (approx. EUR 135,000) for a legal entity, and a fine from HRK 20,000 (approx. EUR 2,650) to HRK 100,000 (approx. EUR 13,500) for the statutory representative of the legal entity. Natural persons may receive a lower fine.

13.5 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 mandatory. However, we recommend notification of a security breach even when there is no explicit legal requirement for such action, especially if by doing so you comply with internationally recognized data privacy principles and standards. This is also advisable because of the general statutory obligation to mitigate potential damage.

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

The main national laws on data protection are the Personal Data Protection Act and the Electronic Communications Act.

13.7 Contact information for Data Protection Authority:

Name:	Agencija za zaštitu osobnih podataka
Address:	Martićeva 14, 10000 Zagreb, Croatia
Telephone:	+385 1 4609-000
Fax:	+385 1 4609-099
Email:	azop@azop.hr
Website:	www.azop.hr

For more information, contact:

Name:	Marija Mušec
Firm:	Odvjetničko društvo Bardek, Lisac, Mušec, Skoko d.o.o. in cooperation with CMS Austria
Address:	Ilica 1, 10000 Zagreb, Croatia
Telephone:	+385 1 4825-600
Fax:	+385 1 4825-601
Email:	marija.musec@bmslegal.hr
Website:	www.bmslegal.hr

14. CZECH REPUBLIC[11]

14.1 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 publicly available electronic communications services. The notification must be made by the publicly available electronic communications services provider ("Provider") who has a direct contractual relationship with the end user. The sub-contractor of the Provider must inform the Provider in case the data breach occurs in the sub-contractor's operations. Providers then must notify:

- The DPA (with a description of the effects of the breach and with measures taken or proposed in reaction to the breach);
- 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 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 Provider to do so and if it has not done so already).

14.2 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 in case of a data breach relating to any personal data;
- The notification obligation is limited to a data breach in relation to the provision of public electronic communications services. According to the DPA, the notification obligation obliges only those Providers who have a direct contractual relationship with the end user (the data subject). It follows that the electronic communications services provider is the data controller, as a data processor should not have a direct contractual relationship with the end user. Data processors have the obligation to notify their customer, i.e., data controllers. The Czech DPA assumes jurisdiction over Providers registered with the Czech Telecommunication Office.

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

14.3 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 done by way of filling in the form published by the DPA on its website. No annexes should be attached to it.

- The notice must be given within 24 hours. If not all information is available to the Provider, further details must be notified as an amendment to the original notification within three days of the first notification. If the Provider still does not have all of the information required, the DPA must be provided with the reasons why all of the required information could not be made available within the three-day deadline.

- The notice can be either submitted electronically via the DPA's form on its website, or email or by mail in printed format or by way of completing and saving the DPA's form on a data storage device (e.g., CD-ROM, USB).

14.4 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 1 million).

14.5 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 standard practice. However, notification is advisable because of the general statutory obligation to limit damage, especially in cases where potential damages could be high.

14.6 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.

14.7 Contact information for Data Protection Authority:

Name:	Urad pro ochranu osobnich udaju
Address:	Pplk 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:	Karin Pomaizlova
Firm:	TaylorWessing e|n|w|c advokati v.o.s.
Address:	U Prasne brany 1, 110 00 Prague 1, Czech Republic
Telephone:	+420 224 81 92 16
Fax:	+420 224 81 92 17
Email:	k.pomaizlova@taylorwessing.com
Website:	www.taylorwessing.com

15. DENMARK[12]

15.1 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)?

The Danish Act on Processing of Personal Data ("APPD") does not include an explicit obligation to notify data subjects in case of a data breach. However, the Danish Data Protection Agency has stated in case law that such notification is necessary, and this requirement follows from the principle of "good practice" under Sec. 5 of the APPD.

There are no requirements to notify the Danish DPA in case of a data breach.

Specific breach notification requirements apply to providers of public electronic communications services (telecommunications providers and internet service providers).

15.2 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?

As a general rule, the data subject must be notified regardless of what types of data are breached, i.e., ordinary personal data, sensitive personal data and semi-sensitive personal data.

The duty of notification rests with the data controller or its representative.

15.3 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 such notices as well as the time period and method for giving them are not further specified in the APPD or any guidance from the Danish DPA.

As a general rule, the data controller or its representative must provide the data subject with the following information in order to comply with the duty of information:

- The identity of the controller and of its representative;
- The purposes of the processing for which the data is intended;
- Any further information which is necessary, having regard to the specific circumstances in which the data is obtained, to enable the data subject to safeguard his/her interests, such as:
  - the categories of data concerned,
  - the categories of recipients, and

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

- the rules on the right of access to and the right to rectify the data relating to the data subject.

Notification to involved individuals must be given as soon as possible and usually within 10 days.

There are no formal requirements as to how the notification shall be given, i.e., whether the notification can be given verbally or in writing. However, for documentation purposes, it is recommended to give the notification in writing.

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

Failure to notify can be sanctioned with a fine or imprisonment up to four months. Furthermore, the data controller may be liable to compensate for any damage caused by the failure to notify.

15.5 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 the event of a 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 damage and prevent future data breaches.

15.6 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, as amended. In addition, the Danish Data Protection Agency has issued a number of guidelines regarding various data protection matters.

15.7 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 3200
Fax:	+45 33 19 3218
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

16. EL SALVADOR

16.1 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 Salvadoran law to notify either affected individuals or any other authority about a data breach. Currently, there is no specialized entity that regulates data protection.

16.2 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.

16.3 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.

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

Not applicable.

16.5 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 specific agreements that include provisions about data breach, risk of dissemination, scope of data involved, magnitude of damage, and measures that may be adopted by the individual to prevent the dissemination or damage.

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

There is no specific Data Protection Law; however, there are certain provisions in other laws that provide a general protection to certain data (personal, sensitive, confidential):

- Consumer Protection Law;
- Intellectual Property Law;
- El Salvador Constitution;
- Law of Computing and Related Crimes;
- Case Law: Supreme Court decisions about data protection; and
- Law for the Regulation of Persons Credit History Services.

16.7 Contact information for Data Protection Authority:

Not applicable.

For more information, contact:

Name: Morena Zavaleta
Firm: Arias & Muñoz
Address: Calle La Mascota #533, Colonia San Benito. San Salvador, El Salvador
Telephone: +503 2257-0900
Fax: +503 2257-0901
Email: morena.zavaleta@ariaslaw.com
Website: www.ariaslaw.com

17. EUROPEAN UNION

This chapter describes the applicable laws and guidelines on the level of the European Union, which form the basis for member state provisions on data protection. With the entry into force of the General Data Protection Regulation (which is expected for 2018), data protection law in the European member states will be governed by that directly applicable regulation, which will leave considerably less room for individual national provisions than is the case today.

17.1 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)?

As of today, there is no general notification requirement under European data protection law in case of a data breach.

Sector-specific legislation

There are, however, sector-specific provisions Directive 2002/58/EC (the so-called "e-Privacy Directive") and Regulation 611/2013.

Pursuant to the e-Privacy Directive, telecoms and internet service providers are obliged to notify the competent national authorities and, in certain cases, also the individuals concerned, of data breaches. To ensure consistency in the implementation of the notification obligation by the EU member states, the European Commission adopted Regulation No 611/2013. This Regulation, which has direct effect in all EU member states, specifies circumstances, format and procedures applicable to these notification requirements under the e-Privacy Directive.

Data breach notification under Directive 95/46/EC

Current European data protection law is based on the Directive 95/46/EC, which was introduced in 1995. The Directive is not directly applicable to persons, bodies or companies processing personal data. EU member states are obliged to implement the provisions of the Directive into their national laws. The Directive does not contain specific provisions on data breach notifications. However, on a national level, several data protection laws require such notification. Please see the respective chapters on the EU member state jurisdictions for further information.[13]

Data breach notification under the draft General Data Protection Regulation

The EU's legislative bodies are currently in the process of preparing an update to European data protection law. The General Data Protection Regulation[14] was agreed in December 2015 and will be formally adopted in the spring of 2016. The Regulation will replace Directive 95/46/EC which

[13] The Guide covers the following EU member states: Austria, Belgium, Croatia, Czech Republic, Denmark, Finland, France, Germany, Greece, Ireland, Italy, Luxembourg, The Netherlands, Poland, Portugal, Slovakia, Slovenia, Spain, Sweden and the United Kingdom.

[14] Latest draft: File ID: 2012/0011 COD, Document No. 15039/15.

is considered to be outdated. Unlike the Directive, the Regulation will be directly applicable in all EU member states (without the requirement of a transposition into national law) and aims at providing greater harmonisation as well as an update of the provisions of the Directive. Its entry into force will be subject to a two-year transition period.

The Draft Regulation includes provisions on data breach notifications to affected individuals and competent authorities.

Data breach notification under the proposed Network Information Security Directive

Data breach notification requirements will also be included in the proposed Network Information Security Directive[15], which is expected to be formally adopted in spring 2016.[16] The proposed Directive aims at ensuring a high common level of network and information security within the EU, and will require operators of essential services (e.g., gas and electric suppliers or healthcare providers) and digital providers (e.g., marketplaces, search engines and cloud computing service providers) to notify the competent national authority of substantial impacts on the provision of their services, i.e., cybersecurity threats. Personal data does not have to be affected to trigger the notification requirement. However, where an incident involves personal data, the notification requirements under the Directive and the Draft General Data Protection Regulation may apply simultaneously.

17.2 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?

e-Privacy Directive

According to the e-Privacy Directive, the requirement only concerns telecoms providers and internet service providers acting as data controllers. Notification must be made in case of breaches of security that lead 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 EU.

Draft General Data Protection Regulation

Under the Draft General Data Protection Regulation, the requirement to notify competent authorities and individuals concerned only applies to data controllers. Data processors are required to immediately inform the respective data controllers. The concept of a data breach appears to remain the same as under the current European legislation.

Data controllers are required to communicate data breaches to individuals in cases where the personal data breach is likely to result in high risks for their rights and freedom, i.e., in physical, material or moral damage.

[15] Document ID: 2013/0027 COD.

[16] The Directive will have to be implemented by the member states into their law within a period of 21 months.

17.3 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?

e-Privacy Directive

Under the current e-Privacy Directive and Regulation 611/2013, telecoms providers and internet service providers are required to notify a data breach to the competent national authority within 24 hours after detection of the breach. If it is not feasible to provide a detailed notification within 24 hours, an initial notification should be made within 24 hours, followed by a detailed notification as soon as possible and within three days of the initial notification. The annexes to the Regulation set out a list of required notification content to the relevant national authority and to subscribers and other individuals who may be adversely affected.

Draft General Data Protection Regulation

Pursuant to the Draft Regulation, notification to the competent authority will have to be made within 72 hours after establishment of a data breach. Following such notification, data controllers are required to communicate the data breach within undue delay to the individuals affected in case such communication is required.

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

e-Privacy Directive

Under the e-Privacy Directive, penalties or fines for noncompliance to the requirements are subject to national law. Please refer to the respective chapters on the EU member states for further information.

Draft General Data Protection Regulation

According to the Draft Regulation, companies that fail to fulfill their data breach reporting obligations may be sanctioned by a fine up to EUR 20 million or, up to 4% of annual worldwide turnover, whichever is greater.

17.5 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)?

Besides the current legal requirement, the Article 29 Working Party (an advisory body on European data protection law consisting of members of the national data protection authorities) published guidance on data breach notification in 2014 encouraging data controllers to notify affected individuals of data breaches even in cases where statutory requirements do not apply. The guidance discusses a wide range of scenarios and gives recommendations regarding procedures and content of (voluntary) data breach notifications. The paper is available for download.

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

See our answer to Question 17.1.

17.7 Contact information for Data Protection Authority:

The competent supervisory authority is the Data Protection Authority of the respective member state.

For more information, contact:

Name: Christian Runte
Firm: CMS Germany
Address: Nymphenburger Straße 12, 80335 Munich, Germany
Telephone: +49 89 238 07 163
Fax: +49 89 238 07 40804
Email: christian.runte@cms-hs.com
Website: www.cms-hs.com

18. FINLAND[17]

18.1 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)?

Finnish law does not recognize any general obligation of data breach notifications.

However, in the context of telecommunications services, if there is a specific violation or a risk of such a violation of the security of information within the service, the telecommunications operator and any "value-added service provider involved" shall immediately notify the users and subscribers. Value-added service providers are defined as providers of a service based on the processing of identification data or location data for a purpose other than the provision of a network service or communications service.

Only the telecommunications operator (and not the value-added 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.

18.2 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 discussed in response to Question 18.1 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 66/2014 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 to a data controller in any other situation.

18.3 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.

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

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 by 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.

18.4 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.

18.5 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.

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

The Information Society Code 917/2014 provides special regulation on confidentiality in electronic communications as well as the handling 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 Code.

18.7 Contact information for Data Protection Authority:

Name: Tietosuojavaltuutetun toimisto
Address: PL 800, 00521, Helsinki, Finland
Telephone: +358 29 566 6700
Fax: +358 29 566 6735
Email: tietosuoja@om.fi
Website: www.tietosuoja.fi

For more information, contact:

Name: Eija Warma or Anette Luomala
Firm: Castrén & Snellman Attorneys Ltd
Address: PO Box 233 (Eteläesplanadi 14), FI-00131 Helsinki, Finland
Telephone: +358 20 7765 376
Fax: +358 20 7761 376
Email: eija.warma@castren.fi or anette.luomala@castren.fi
Website: www.castren.fi

19. FRANCE[18]

19.1 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 the French data protection authority ("CNIL") and the affected individuals of a data breach but only under certain conditions related to public electronic communications services (see below).

19.2 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 unauthorised 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 available electronic communication services need to be reported, regardless of the severity.

19.3 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 notify the personal data breach to the CNIL within 24 hours of becoming aware of the breach.

If it is not possible to provide all information required within this time frame (e.g., further investigation is required), notice may be given in two stages: (1) initial notice within 24 hours of the breach; and (2) supplementary notice within 72 hours of the initial notice.

The CNIL has now implemented an online breach reporting mechanism on its website, www.cnil.fr.

While there is no strict legal requirement regarding the method of giving notice, the new online breach reporting mechanism now means that notice should be given using the notice form that may be downloaded from the CNIL's website. The notice form may be completed and submitted online or sent by post. If sending by post, it is recommended to use certified mail with a return receipt requested.

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

The notification to the CNIL shall contain the following information:

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

On the latter point, the provider must provide an explanation of whether it has notified the individuals concerned and, if not, the reasons for the lack of notification or delay, i.e.:

- That appropriate measures of protection have been implemented (see below); or
- That it considers that the notification to the subscribers or individuals may put at risk the proper investigation of the personal data breach; or
- That it was unable to identify all the individuals concerned within the timeframe and has attempted to inform these individuals through advertisements in major national or regional media while continuing to try to identify them in order to notify them individually as soon as possible.

In principle, the provider must notify the individual of the breach without delay only if the personal data breach is likely to adversely affect the personal data or privacy of the individual.

However, notification to the individual is not necessary if the CNIL has decided that appropriate measures of protection have been implemented to render the data unintelligible to any person who is not authorised 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. A full description of the measures has to be provided in the notification to the CNIL to enable the CNIL to assess them.

The notification to the individual shall contain the following information:

- The nature of the personal data breach;
- The identity and contact details of the individuals who can provide additional information; and
- The measures recommended by the provider to moderate the negative consequences of the breach.

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

The CNIL will make a decision 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 a timeframe it specifies, usually within one month.

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

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

19.5 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 of 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.

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

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

19.7 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 1 5373 2222
Fax:	+33 1 5373 2200
Email:	See website
Website:	www.cnil.fr

For more information, contact:

Name:	Laure Marolleau
Firm:	Soulier Avocats
Address:	50 Avenue de Wagram, 75017 Paris, France
Telephone:	+33 1 4054 2929
Fax:	+33 1 4054 2920
Email:	l.marolleau@soulier-avocats.com
Website:	www.soulier-avocats.com

20. GERMANY[19]

20.1 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 or "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.

20.2 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 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).

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

20.3 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 minimize possible harm include information on available technical security measures such as patches, other security software and/or updates, and recommendations on changing passwords. Data subjects shall be informed as soon as appropriate that measures to safeguard the data have been taken and notification would no longer pose a risk to 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 entity 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 measures for notifying data subjects.

20.4 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 EUR 300,000 and the fine should exceed the financial benefit to the perpetrator derived from the offence. If EUR 300,000 is not sufficient to do so, this figure may be increased.

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

20.5 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.

20.6 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).

20.7 Contact information for Data Protection Authority:

Offences have to be notified respectively with the competent state supervisory authorities for the non-public sector. The competent authority will have to be determined in the individual case based on the place of business of the respective company. An overview of the most recent contact details for all state authorities is currently available here.

For more information, contact:

Name: Christian Runte
Firm: CMS Germany
Address: Nymphenburger Straße 12, 80335 Munich, Germany
Telephone: +49 89 238 07 163
Fax: +49 89 238 07 40804
Email: christian.runte@cms-hs.com
Website: www.cms-hs.com

21. GREECE[20]

21.1 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 Act on 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 the 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 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.

21.2 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.

21.3 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 the 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 contacts from whom 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 or form of giving notice.

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

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

Pursuant to Law 3115/2003 article 11, in case of a breach of privacy in the telecommunications sector or the revocation of its terms and procedures, 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 ranging between EUR 15,000 and EUR 1,500,000.

These administrative sanctions shall only be imposed following the issuance of a substantiated decision of 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, 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 EUR 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 above 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 year and a fine of between EUR 10,000 and EUR 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 EUR 12,000 and EUR 120,000;
- If perpetrators 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 between EUR 15,000 and EUR 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 EUR 50,000 and EUR 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 EUR 10,000.

21.5 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 advisable even though it is not required by law.

21.6 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.

21.7 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:	contact@dpa.gr
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

22. GUATEMALA

22.1 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 Guatemalan law to notify either authorities or affected individuals. There is not a specific Data Protection Authority in Guatemala.

22.2 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.

22.3 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.

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

Not applicable.

22.5 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 analysed on a case-by-case basis when deciding whether to notify an individual of a data breach. Key points of consideration include the magnitude of damage and measures that may be adopted by the individual to prevent the dissemination or prevent any further damages.

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

- Article 24 of the Constitution of the Republic of Guatemala protects private correspondence, documents and books;
- Access to Public Information Act Decree 57-2008 of Congress of which:

(a) Article 9 section 2 defines personal data as all data related to an identifiable individual,

(b) Article 9 section 3 defines personal sensitive data as data regarding physical aspects, moral, personal habits, ethnic characteristics, health, ideology, political opinions, religion and other intimate aspects,

(c) Article 22 classifies sensitive data as confidential information, and

(d) Article 64 prohibits and penalizes commercialisation and distribution of personal data and personal sensitive data unless the information is from a public registry or the individual has granted his/her prior written express consent.

- Article 6 Section (j) of the People's National Registry Act classifies home address as restricted personal data; and
- Article 274 "D" of the Criminal Code Decree 17-73 of Congress proscribes the creation of illicit records in respect to records related to information that might affect people's privacy.

22.7 Contact information for Data Protection Authority:

Not applicable.

For more information, contact:

Name: Pamela Jiménez
Firm: Arias & Muñoz
Address: Diagonal 6, 10-01 zona 10 Centro Gerencial Las Margaritas, Torre II, oficina 402-B. Ciudad de Guatemala, Guatemala, C. A.
Telephone: +502 2382 7700
Fax: +502 2382 7743
Email: pamela.jimenez@ariaslaw.com
Website: www.ariaslaw.com

23. HONDURAS

23.1 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 Honduras law to notify either the affected individuals or the Institute of Access to Public Information ("IAIP") of a data breach. Please note that there is no special law on data protection and privacy; the only relevant law is the Law on Transparency and Access to Public Information and its Regulation, which are applicable to governmental entities. There are also certain dispositions related to the matter in the Constitution and the Code of Commerce. [21]

Currently, there is a motion at the National Congress to approve a General Data Protection and Privacy Law.

23.2 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.

23.3 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.

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

Not applicable.

23.5 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, it is recommended. Considering that the Law on Transparency and Access to Public Information demands that a written consent from the person is necessary for the transfer of personal data (and we recommend this for all data transfer operations), we would recommend notifying the person in case the information he or she authorised to be transferred is breached.

[21] Article 956 of the Code of Commerce: Banking institutions may not disclose information of deposits and other operations except to the depositor, debtor or beneficiaries, legal representatives or whoever has the power to dispose of the account or to intervene in its operation except in those cases when through a court order information is requested of the depositor.

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

As mentioned above, there is no special data protection law. In a more general manner, the following laws regulate data use matters and may be of interest:

Constitution:

- Art. 76: Guarantees honour, personal and familiar intimacy;
- Art. 100: Every person has the right to the inviolability and secrecy of communications, especially postal, telegraphic and telephonic communications except when there is a court ruling ordering the contrary. Corporate and personal documents may only be subject to inspection or supervision by competent authorities, as permitted by law; and
- Art. 183: Establishes "garantia de amparo" as an action for the protection of an individual's constitutional rights.

Penal Code:

- Art. 214: Penalizes those who seize personal information through any means.

Law on Transparency and Access to Public Information: Gives the right to individuals to access public information of public entities.

Law of the National Registry of Persons (Ley del Registro Nacional de las Personas): States that the information of the Registry is public; however, its accessibility and disclosure will be restricted in cases when its use may affect the image, honor and privacy of an individual and/or family.

Code of Commerce:

- Art. 956: Banking institutions may only disclose information of deposits and other similar operations to the depositor, debtor or beneficiaries, or their legal representatives who have the power to dispose of the account or to intervene in its operation.

Financial System Law:

- Art. 34: Members of the board of directors, general managers and other employees of an institution of the financial system can incur responsibility if they disclose or divulge any confidential information on matters related to the banking institution.

Regulation for the Authorization and Functioning of Private Credit Bureaus:

- Art. 3: Establishes that the provision of services consistent in the compilation, management and delivery of information related to the credit history of the information holders, as well as the credit operations and others of similar nature, be maintained with the supervised and non-supervised institutions of the CNBS (Banking Regulator), and may only be carried out by

institutions incorporated as fixed capital corporations (Sociedad Anonima de Capital Fijo). Their corporate name must indicate their status as private credit bureaus, and for the effect of their incorporation and operation require authorization from the CNBS.

- Art. 19: Also establishes that the databases that these kind of companies keep must be located within the national territory.

- Art. 22: Dictates that the direct transfer of credit information or any other information to companies, public and private institutions, natural and judicial persons in other countries, or international or supranational/multinational organisations is prohibited if these companies are not users. Users, according to the regulation, are people or corporations that request information from the bureau, through prior written authorization, extended by the holder of the information.

Norms to regulate the Administration of the Technology of Information and Communications in the Institutions of the Financial System:

- Art. 38: Reads that financial institutions may hire an external entity to carry out the following activities: the administration processing and backup of information operations, as well as development of its systems, consulting services, patents and other related services.

- The process of hiring third parties to carry out these kinds of services must be made with knowledge from CNBS, prior the subscription of the following contracts:

  (1) Outsourcing of central systems; and

  (2) Storage of information of any type, in relation to clients of the institution, in systems that are not in its exclusive control.

- CNBS may make observations on the security, trustworthiness and efficiency of the services to be rendered. CNBS may also assess experience, capacity and economic viability of the service provider. These kinds of services are considered essential to banking institutions and and must be complied with prior to the subscription of service contracts.

Special Law on the Intervention of Private Communications

Due to the current security issues arising in Honduras, Congress approved this law that allows the intervention of certain communications when it is believed it could serve a criminal investigation. The Law dictates a process for the approval of the intervention by a judge.

23.7 Contact information for Data Protection Authority:

Name:	Instituto de Acceso a la Información Pública
Address:	Col. Tepeyac, Edificio Panorama, costado Sur del hospital Honduras Medical Center, calle de acceso entre el antiguo local del Restaurante La Pimentera y el antiguo local del Banco Procredit, penúltimo cubículo del lado izquierdo.
Telephone:	+504 2231 3162
Email:	marcela.sarmiento@iaip.gob.hn
Website:	www.iaip.gob.hn

For more information, contact:

Name:	Mario Agüero
Firm:	Arias & Muñoz
Address:	San Pedro Sula, Edificio Park Plaza, Local 19, Barrio Guamilito, 5° y 6° Calle, 11 Avenida N.O. San Pedro Sula, Cortes, Honduras
Telephone:	+504 2550-2202
Fax:	+504 2557-6488
Email:	mario.aguero@ariaslaw.com
Website:	www.ariaslaw.com

24. INDIA

24.1 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)?

Generally, a data breach is not required to be reported. India does not have a DPA.

However, if there is a cybersecurity incident, any individual, organisation, or corporate entity affected by the cybersecurity incident may report such incident to the Indian Computer Emergency Response Team ("CERT-In").

"Cybersecurity incident" means any real or suspected adverse event in relation to cybersecurity that violates an explicitly or implicitly applicable security policy resulting in unauthorised access, denial of service or disruption, unauthorised use of a computer resource for processing or storage of information or changes to data or information without authorization.

Certain types of cybersecurity incidents require mandatory reporting. Cybersecurity incidents that require mandatory reporting are discussed in the response to Question 24.2 below.

There is no requirement to notify affected individuals.

24.2 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?

Cybersecurity incidents that must be reported are:

- Targeted scanning/probing of critical networks/systems;
- Compromise of critical systems/information;
- Unauthorised access of IT systems/data;
- Defacement of a website or intrusion into a website and unauthorised changes such as inserting malicious code, links to external websites, etc.;
- Malicious code attacks such as spreading of virus/worms/trojans/botnets/spyware;
- Attacks on servers such as database, email and DNS and network devices such as routers;
- Identity theft, spoofing and phishing attacks;
- Denial of service (DoS) and distributed denial of service (DDoS) attacks;

- Attacks on critical infrastructure, SCADA Systems and wireless networks;
- Attacks on applications such as E-governance, E-commerce, etc.

Both the data controller and the data processor have the obligation to report.

24.3 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 incident can be reported in the format available on the website: cert-in.org.in.

(a) Contents to be reported include: (i) time of occurrence; (ii) symptoms; (iii) information regarding affected system or network, etc.

(b) The incident must be reported as early as possible.

(c) The incident can be reported by:

e-mail to: incident@cert-in.org.in
help desk: +91 18 0011 4949
fax: +91 18 0011 6969

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

Failure to file the information may result in penalty of INR 5,000 (approx. USD 100) for each day of failure.

24.5 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 notification to the affected individual is required unless it is desirable to notify the individuals so they can take action to minimize the impact of the data breach.

24.6 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") promulgated 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, possesses, 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 corporate entity regarding usage, collection and transfer of personal information and implementation of reasonable security practices.

Further, the Information Technology (the Indian Computer Emergency Response Team and Manner of Performing Function and Duties) Rules, 2013 deal with reporting of cybersecurity incidents and dealing with the same.

Apart from the above, there are provisions relating to protection of privacy in telecom regulations, banking and financial regulations to a certain extent.

24.7 Contact information for Data Protection Authority:

Not applicable

For more information, contact:

Name:	Bomi Daruwala
Firm:	Vaish Associates Advocates
Address:	106, Peninsula Centre, Dr. S. S. Rao Road, Parel, Mumbai – 400012
Telephone:	+91 22 4213 4101
Fax:	+91 22 4213 4102
Email:	bomi@vaishlaw.com
Website:	www.vaishlaw.com

25. INDONESIA

25.1 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)?

Indonesia does not yet have a consolidated or comprehensive law on data privacy or data protection. The main law and regulation that regulates data protection is Law No. 11 of 2008 on Electronic Information and Transactions and Government Regulation No. 82 of 2012 on The Implementation of Systems and Electronic Transactions. These cover non-paper based documents and information as well as electronic transactions, i.e., data that is held electronically.

Art. 15 (1) of Government Regulation No. 82 of 2012 obliges Electronic System Operators ("ESO") to protect the confidentiality, integrity and availability of the private data they manage. In the event of failure to protect data, which may include a data breach, the ESO must notify the owner of the data in writing. There is no obligation under Law No. 11 of 2008 or Government Regulation No. 82 of 2012 to notify the regulator of any data breach.

In addition to the above laws and regulations, data protection and/or data privacy are also provided for in certain industry-specific laws and regulations covering, for example, the health, telecommunications and banking sectors.

25.2 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?

As explained above, the ESO must notify the owner of the private/personal data of any breach. This applies to ESOs in general. An ESO is defined as any private person, state operator, enterprise, or element of society who makes available, manages, and/or operates an electronic system either privately or communally for the electronic system's users for his/her own benefit, or a third party's benefit.

25.3 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?

Government Regulation No. 82 of 2012 is silent on the content of the notice or time limit within which the notice must be given. It only provides that the notice should be in writing.

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

Government Regulation No. 82 of 2012 is silent on any penalties or fines for failing to make such a notification.

25.5 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 explained in our answer to Question 25.1. above, the obligation to notify the owner of the data is imposed under Government Regulation No. 82 of 2012. We would recommend notifying the data owner anyway as this will limit the potential damage or loss that third parties may suffer as a result of the data breach. It would also give an opportunity to the relevant parties to take further measures to settle any claims or grievances.

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

As explained in our answer to Question 25.1. above, currently, Indonesia does not have a comprehensive data protection law or guidelines. A draft regulation on personal data protection has been prepared by the Indonesian Ministry of Communications and Informatics. However, it is unlikely that the regulation will be issued before 2016 due to its absence from the 2015 Prolegnas (Indonesian National Legislative Program).

Laws and regulations that currently directly or indirectly provide for data protection in Indonesia include:

- Law No. 11 of 2008 on Electronic Information and Transactions;
- Law No. 7 of 1992 on Banking as amended by Law No. 10 of 1998;
- Law No. 36/2009 on Health;
- Law No. 36/1999 on Telecommunications;
- Law No. 14 of 2008 on the Disclosure of Public Information;
- Government Regulation No. 82 of 2012 on the Management of Electronic Systems and Transactions;
- Bank Indonesia Regulation (PBI) No. 16/1/PBI/2014 on Consumer Protection in Payment System Services; and
- Financial Services Authority (Otoritas Jasa Keuangan/"OJK") Regulation No. 1/POJK.07/2013 on Consumer Protection in Financial Services.

25.7 Contact information for Data Protection Authority:

The Government of the Republic of Indonesia has not established a specific Data Protection Authority. General inquiries on this matter can be submitted to the Ministry of Communications and Informatics.

Name:	Ministry of Communications and Informatics of the Republic of Indonesia
Address:	Jl. Medan Merdeka Barat No. 9, Jakarta, Indonesia 10110
Telephone:	+62 213452841
Email:	humas@mail.kominfo.go.id
Website:	www.kominfo.go.id

For more information, contact:

Name:	Richard Cornwallis
Firm:	Makarim & Taira S.
Address:	Summitmas I, 16th & 17th floors, Jl. Jend. Sudirman Kav. 61-62, Jakarta, Indonesia 12190
Telephone:	+ 6221 252 1272, 520 0001
Fax:	+6221 252 2750, 252 2751
Email:	richard.cornwallis@makarim.com
Website:	www.makarim.com

26. IRELAND[22]

26.1 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 Personal Data Security Breach Code of Practice (the "Code"), which applies to all data controllers and data processors; and (ii) the Privacy and Electronic Communications Regulations 2011 (the "Regulations"), which apply to certain entities in the telecommunications sector.

The Code is not legally binding, though the Data Protection Commissioner (the "DPC") may argue that it reflects the requirements implicit from the fair processing principle.

The Data Protection Acts 1988-2003 (the "Irish DPA") impose a number of broad and general obligations on data controllers. These include the obligation to process data "fairly" (Section 2(1)(a) and 2D of the Irish DPA) and to deploy "appropriate" security measures to protect the data (Section 2(1)(d) and 2C of the Irish DPA). The DPC may argue that the Code is reflective of these general principles of data protection law.

- Notification 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.

  Separately, 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.

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

- Notification to Regulator

Under the Code, all incidents in which personal data has been put at risk should be reported to the DPC, 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 DPC where there is a personal data breach.

26.2 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?

- Who must notify under the Regulations

Under the Regulations, it is stated that the "undertaking" (i.e., provider of an electronic communications service or network) shall notify of the breach.

- Who must notify under the Code

Under the Code, the obligation is on the data controller to notify the affected subjects. 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.

- What types of data trigger notification

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.

See response to Question 26.1 for further detail in relation to when the obligation is triggered.

26.3 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 may be given by email, telephone or fax.

- Notification under the Code

The Code provides that the notification to the DPC 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.

- Notification under the Regulations

Under the Regulations, a notification, to both the affected individual and the DPC, 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 DPC, a description of the consequences of, and the measures proposed to be taken by the undertaking to address, the personal data breach.

Under the Regulations, notice should be given "without undue delay."

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

- Position under the Code

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 DPC 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.

- Position under the Regulations

Under the Regulations, an undertaking may be liable for a fine of between EUR 4,000 and EUR 250,000 (for a corporate entity) or EUR 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 DPC may, having considered the likely adverse effects of the breach, require the undertaking to do so by serving an enforcement notice.

- Enforcement notices

The DPC has, in the past, taken formal enforcement action so as to force companies to make notifications following data breaches. For example, in *"Data Security Breach at Loyaltybuild Ltd: Case Study 14 of 2013"*, a case concerning a major security breach of personal data of some 1.5 million individuals (including 376,000 individuals whose full credit card data was compromised), the DPC issued enforcement notices against a number of data controllers directing them to notify the affected individuals.

Non-compliance with an enforcement notice is a criminal offence and the DPC can issue an enforcement notice where there has been a contravention of the Irish DPA. In contrast, a contravention of a mere non-binding code of practice does not provide grounds for the issuance of an enforcement notice.

In addition, an enforcement notice can direct the taking of steps where such steps are necessary for the recipient to comply with the Irish DPA, but not where such steps are necessary for compliance with a non-binding code of practice. In other words, the DPC has previously taken formal enforcement action against companies on the basis that non-notification, following a security incident, constitutes a breach of the Irish DPA, and not just the Code.

Failure to comply with an enforcement notice is a criminal offence under the Irish DPA.

Criminal prosecutions for breaches of the Irish DPA are relatively rare and when brought have often concerned a failure to register. Summary proceedings may be brought by the DPC, while prosecution on indictment requires the cooperation of the Director of Public Prosecutions.

A person summarily convicted of a breach of the Irish DPA is subject to a fine of up to EUR 3,000 which conviction on indictment is subject to a fine of up to EUR 100,000.

Even in cases that have not risen to the level of formal enforcement action, the DPC has taken the line that individuals should be notified of security breaches where their personal data has been compromised. For example, in *"Lost Passports: Case Study 16 of 2013"*, a case involving the loss of photocopies of passports by a voluntary organisation that is involved with young people, the DPC noted that "[t]he three-pronged approach from this Office when dealing with personal data security breaches is that we expect the Data Controller…(1) informs the affected individuals (including what information was disclosed)".

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

- Damages

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.

Under section 7 of the Irish DPA, both data controllers and data processors owe a duty of care to the data subject. This duty of care means that the data subject is entitled to sue under the law of torts in the event of a breach of that duty of care.

In the majority of cases the type of loss suffered in a breach of privacy and data rights is one of moral damage, or distress, rather than identifiable pecuniary loss.

In the case of *Collins v FBD Insurance* [2013] IEHC 137, the plaintiff argued that he was entitled to recover damages where there was a breach of duty by the data controller or data processor, even where the data subject incurred no actual damage. The High Court rejected this claim and found that to succeed in a claim for damages under s. 7 of the Irish DPA the plaintiff must be able to prove actual damage. This suggests that the tort under s. 7 of the Irish DPA is in line with the general principles of the tort of negligence.

This case was decided before the UK *Vidal-Hall v Google* case where it was held that there is no requirement to suffer pecuniary loss to recover damages in respect of distress in a data protection context. Whilst UK case law is not legally binding on the Irish Courts, it can be of persuasive authority. Consequently, it cannot be ruled out that an Irish Court could reconsider the approach taken in *Collins v FBD Insurance* having regard to *Vidal-Hall*. The *Vidal-Hall* case is being appealed.

26.5 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.

26.6 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;
- European Communities (Electronic Communications Networks and Services);
- (Privacy and Electronic Communications) Regulations 2011; and
- Data Protection Acts 1988 and 2003.

26.7 Contact information for Data Protection Authority:

Name:	Office of the Data Protection Commissioner
Address:	Canal House, Station Road, Portarlington, Co. Laois, Ireland
Telephone:	+353 1 57 868 4800
Fax:	+353 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

27. ISRAEL

27.1 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 statutory/regulatory requirement under Israeli protection of privacy laws to notify the affected individuals or the DPA of a data breach affecting an Israeli resident. There might be such requirements under specific legislation applicable to specific fields. This should be reviewed and confirmed on a case-by-case basis and we do not refer to these possible matters in this chapter.

27.2 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.

27.3 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.

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

Not applicable.

27.5 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 is something that should be considered regardless of there being no general statutory/ regulatory requirement to do so under the protection of privacy laws in Israel, in order to reduce possible damages and exposure under tort and contract law, if in the applicable circumstances such damages might exist.

27.6 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.

27.7 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:	+972 2 646 7064
Email:	ILITA@justice.gov.il
Website:	www.justice.gov.il/MOJEng/RashutTech/default.htm

For more information, contact:

Name:	Nurit Dagan
Law firm:	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

28. ITALY[23]

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

Yes, but only for:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

The main data protection national laws and regulations are:

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

28.7 Contact information for Data Protection Authority:

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

For more information, contact:

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

29. JAPAN

29.1 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)?

Protection of personal information is mainly regulated under the Act on the Protection of Personal Information (APPI). The APPI does not have any clause that specifically sets forth that notice must be given to affected individuals or regulators. However, Article 20 of the APPI sets forth that a business operator handling personal information must 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 20, the entity that committed a data breach may be legally obliged to notify individuals who may be affected by such data breach. Various ministries and government agencies have issued guidelines on the protection of personal information for the fields they supervise. While one guideline differs from another, many of the guidelines require or recommend prompt reporting to the supervising authority, giving notice to the affected individuals, and making public announcement of the relevant facts and preventative measures for recurrence.

Recently on 3 September 2015, a bill to amend the APPI and the Act on the Use of Numbers to Identify a Specific Individual in the Administrative Procedure (which is known as the "My Number Act") passed the Diet. The new Article 28-4 of the amended My Number Act provides that the person in charge of affairs using "My Number" and certain other information must report to the Personal Information Protection Committee ("Committee") in case of a breach of specific personal information (including "My Number"), in accordance with the Committee Rules. The Committee is currently expected to be established in January 2016 and to issue the Committee Rules at a later date. "My Number" is a number that will be assigned to individuals for purposes such as tax and social welfare.

29.2 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, but many of the ministry and agency guidelines require notice when personal information in general is breached, without specifying what type of data. It is interpreted that the scope of the APPI is limited to handling of personal information within Japan, in principle, and data processors' handling personal information only outside of Japan are not subject to APPI.

29.3 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?

This will also depend on the relevant guidelines, but many of the guidelines provide that notices be given promptly, without providing any specific time limit, method or content. Many of the guidelines provide that the purposes of these notices are to prevent secondary damages and similar incidents.

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

The supervising authority can issue a recommendation in case of a violation of the obligation to take necessary and proper measures for the security control of personal data under Article 20 of the APPI. If this recommendation is not complied with absent legitimate grounds, the authority can give an order to the same effect. Violation of such an order will be subject to imprisonment of up to six months or a fine of up to JPY 300,000.

With respect to a violation of the obligation to report a breach of specific personal information to the Committee under the My Number Act, the Committee can make a recommendation to cure the violation. If the recommendation is not followed without a legitimate ground, the Committee can give an order to the same effect. Violation of such order will be subject to imprisonment of up to two years or a fine of up to JPY 500,000.

29.5 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 is recommended in order to minimize any possible damages.

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

The main data protection law is the Act on the Protection of Personal Information (APPI).

In addition, as of 1 September 2015, 38 guidelines have been issued by various ministries and government agencies in relation to 27 fields in the private sector.

29.7 Contact information for Data Protection Authority:

Name: Consumer Affairs Agency (responsible for general legal framework only)
Address: Sanno Park Tower, 2-11-1, Nagatacho, Chiyoda-ku, Tokyo, Japan
Telephone: +81 3 3507-8800
Website: www.caa.go.jp

The current roles and authorities of various supervising ministries and government authorities (including the Consumer Affairs Agency) in relation to the APPI will be consolidated to the Personal Information Protection Committee, which is scheduled to be established in January 2016.

For more information, contact:

Name: Hitoshi Sakai
Firm: City-Yuwa Partners
Address: Marunouchi Mitsui Building, 2-2-2 Marunouchi, Chiyoda-ku, Tokyo, Japan, 100-0005
Telephone: + 81 3 6212 5642
Fax: + 81 3 6212 5700
Email: hitoshi.sakai@city-yuwa.com
Website: www.city-yuwa.com

30. LUXEMBOURG[24]

30.1 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 (i) any imminent risk of breach of the security of the network or services that may compromise the confidentiality of communications and (ii) of any data breach that is likely to negatively affect the personal data or privacy of the subscriber or individual.

There is also a legal obligation to notify the DPA but only under certain conditions related to electronic communications services providers.

30.2 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 unauthorised access to personal data that is being transmitted, stored or otherwise processed in connection with the provision of publicly available electronic communications services".

The obligation to notify the DPA only applies to providers of publicly available electronic communication services.

30.3 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 service provider of publicly available electronic communication services must notify the data breach without delay. The terms "without delay" are interpreted by the DPA as meaning within 24 hours from the findings of the breach.

If it is not possible to gather all the information required within this timeframe, the DPA provides that notice may be given in two stages: (1) initial notice within 24 hours and (2) supplementary notice within three days following the initial notice. To the extent the second timeframe (i.e. within three days following the initial notice) cannot be complied with, the service provider must present a valid justification regarding the reason for such impossibility and provide the missing information to the DPA as soon as possible.

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

The DPA has now implemented an online breach notification mechanism on its website via a specific form: www.cnpd.lu.

While the law does not set out the requirements regarding the method of giving notice, the notification form may be completed and submitted online, by facsimile or by registered mail.

As regards the content of the notice, the law indicates that, in the context of the notification to the subscribers or to data subjects concerned by the data breach, the service provider of electronic communications must at least indicate the nature of the breach, the contact details where additional information may be obtained and some recommendation to reduce the negative consequences of the breach.

In addition to these elements, the DPA provides on its website that the following information must also be communicated to subscribers and data subjects concerned by the data breach:

- The name of the service provider;
- A summary of the incident which resulted in the data breach;
- The estimated date of the incident;
- The nature of the personal data concerned by the breach;
- The possible consequences of the breach for the subscribers or data subjects concerned;
- The circumstances of the breach;
- The measures undertaken by the service provider to remedy the breach; and on an optional basis:
  - The content of the notification;
  - The communication means that were used; and
  - The number of subscribers or data subjects concerned.

As regards the information to be communicated to the DPA, the law provides that, in addition to the legally required information provided to subscribers and data subjects, the notification must state the consequences of the data breach and the appropriate measures undertaken or proposed by the service provider to remedy the breach.

In addition to these elements, the DPA provides on its website that the following information must also be communicated:

- The exact (or if unknown, the estimated) date and time of the incident and the date and time when the incident was reported;
- The circumstances of the data breach (such as loss, theft, etc.);
- The nature of the personal data concerned by the breach;
- The technical and organisational measures implemented or to be implemented by the service provider;
- Whether the service provider has used the service of any other third-party providers;
- A summary of the incident that resulted in the data breach (including information as regards the physical location of the breach);
- The number of subscribers or data subjects concerned;
- The possible consequences and/or damages for subscribers and/or data subjects; and
- The technical and organisational measures undertaken by the service provider to remedy the breach.

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

Repeated failures by service providers to notify the DPA despite warnings received from the DPA entitles the latter to impose fines of up to EUR 50,000.

To the extent the security breach is caused by an absence of appropriate security and organisational measures, this may constitute an infringement of the Luxembourg data protection law and/or the Luxembourg law relating to the processing of personal data in the electronic communications sector as further described below, which, as such, may be subject to criminal sanctions (fines of up to EUR 125,000 and/or imprisonment of up to one year), civil sanctions in the form of damages and/or administrative sanctions (warnings, temporary or permanent ban on the data processing, orders to delete or destroy data that have been subject to processing in breach of the legal provisions).

30.5 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 advisable to inform the data subjects in the event of data breaches that may affect their personal data even if there is no general mandatory obligation to notify affected persons.

30.6 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, as amended; 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, as amended.

30.7 Contact information for Data Protection Authority:

Name:	Commission nationale pour la protection des données (National Commission for Data Protection)
Address:	1, avenue du Rock'n'Roll L-4361 Esch-sur-Alzette Grand-Duchy of Luxembourg
Telephone:	+352 26 1060 1
Fax:	+352 26 1060 29
Email:	info@cnpd.lu
Website:	www.cnpd.lu

For more information, contact:

Name:	Héloïse Bock
Firm:	Arendt & Medernach S.A.
Address:	41A, avenue J.F. Kennedy, L-2082 Luxembourg
Telephone:	+352 40 7878 321
Fax:	+352 40 7804 609
Email:	heloise.bock@arendt.com
Website:	www.arendt.com

31. MALAYSIA

31.1 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)?

Malaysia's Personal Data Protection Act 2010 ("PDPA"), which came into force on 15 November 2013, does not contain a provision that mandates a data processor or data user to notify a data subject or data protection authority of a data breach.

However, financial institutions are required to comply with the Guidelines on Data Management and MIS Framework (BMN/RH/GL-018-1, "Circular") issued by the Malaysian Central Bank. The Guidelines require financial institutions in Malaysia to establish and maintain a sound data management and management information system and sets out certain guiding principles on the same.

The Circular also provides that any system deterioration observed in data quality should be investigated by the affected financial institutions and reported to the Board of Directors of the financial institution for risk management. The Board must promptly inform the Central Bank of "any developments that may have a material bearing on the institution's operations, risk profile or financial condition."

31.2 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 under the PDPA.

For financial institutions, please refer to the answer to Question 31.1.

31.3 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.

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

Not applicable.

31.5 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. However, it is necessary to consider the nature and extent of the breach on a case-by-case basis. Notifying affected data subjects of a data breach may be a relevant consideration for the courts in determining the quantum of civil damages.

31.6 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; and
- Credit Reporting Agencies Act 2010.

31.7 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

32. MÉXICO

32.1 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 Art. 20 of the Federal Law for the Protection of Personal Data in Possession of Private Parties ("Mexican Data Protection Law") and Art. 64 of the Regulations of the Mexican Data Protection Law ("Regulations"), any security breach significantly affecting the financial and moral rights of the data subject requires notification by the data controller to such data subject. No notification is required to the DPA.

The data subject does not need to be a national of Mexico, but only an individual whose personal data is protected under the Mexican Data Protection Law. Therefore, the Mexican Data Protection Law may be applicable to a controller located outside of Mexico.

32.2 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 Mexican Data Protection Law and its Regulations do not specify 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 triggers a requirement to notify.

The notification must be given by the controller upon 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 actions intended to analyse the extent of the breach.

32.3 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 Art. 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.

The Mexican Data Protection Law provides that the controller must immediately notify data subjects upon confirmation of a data breach and, once it has taken those actions, to analyse the effect on the data subjects. Mexican Data Protection Law and its Regulations do not establish a particular method to give a data breach notice; however, it is advisable to use a method that would allow data subjects to effectively be informed of the breach.

32.4 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 analysis on a case-by-case basis, failure to notify the data subject may be deemed by the National Institute of Transparency, Information Access, and Personal Data Protection ("INAI") as a breach to the data protection principles provided by the Mexican Data Protection Law.

Accordingly, the INAI may impose a fine between 100 to 160,000 times the Unit for Measure and Update that is published by the National Institute of Statistics and Geography (currently, between MXN 7,304 and MXN 11,686,400). Penalties may double if the breach involves sensitive personal data. The above are in addition to any civil or criminal liabilities that may arise from the data breach and any damages caused to the data subject.

32.5 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 notification of a security breach, even if it is not mandatory under the Mexican Data Protection Law, to reduce or limit any possible damage to the data subject resulting in the controller being liable under civil or criminal law. It should be considered that the notice delivered to the data subject may be considered as acknowledgement of a breach in law and may, therefore, be used by the data subject as evidence in an attempt to file a civil claim demanding indemnification of damages resulting from an unlawful act.

32.6 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 Private Entities;
- Regulations of the Federal Law for the Protection of Personal Data in Possession of Private Entities;
- Guidelines of the Privacy Notice; and
- Sectoral laws (e.g. General Law on Health, Regulations of the General Law on Health Investigation, among others).

32.7 Contact information for Data Protection Authority:

Name:	National Institute of Transparency, Information Access, and Personal Data Protection
Address:	Insurgentes Sur No. 3211, Colonia Insurgentes, Cuicuilco, Delegación Coyoacán, Zip Code 04530, Distrito Federal, México
Telephone:	+52 01 800 8354324
Email:	atencion@ifai.org.mx
Website:	http://inicio.ifai.org.mx/SitePages/ifai.aspx

For more information, contact:

Name:	César G. Cruz Ayala or Diego R. Acosta Chin
Firm:	Santamarina y Steta
Address:	Ricardo Margain Zozaya 335, Piso 7, Col. Valle del Campestre, 66265 San Pedro Garza García, N.L., (Monterrey) México
Telephone:	+52 81 8133 6002 or +52 81 8133 6018
Fax:	+52 81 8368 0111
Email:	ccruz@s-s.mx or dacosta@s-s.mx
Website:	http://www.s-s.mx/site/eng

33. MONGOLIA

33.1 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 the Law of Mongolia "On Personal Secrecy" dated 21 April 1995 (as amended), "personal sensitive information" means communications, health, property, family and any other secrets defined by law. Any person who has become aware of the personal sensitive information of an individual pursuant to the law, or under any power of attorney, are prohibited from disclosing such information. If this restriction on disclosure is breached, the sanction may be either a fine or imprisonment for the person in charge of that organisation's confidentiality or the person to whom the sensitive information is disclosed due to their duties and in the course of performing their work.

In the event of a data breach, there is currently no legal obligation to notify the affected individual. However, an obligation or requirement to notify an individual in the event of a data breach may be included under an internal regulation of any organisation. The Law of Mongolia on Organisational Confidentiality (1995) allows all organisations to adopt internal regulations on the protection of an organisation's confidential information, and imposes obligations on organisations to protect personal sensitive information that has become available to each organisation during the course of its operations, as its own confidential information.

In Mongolia, there is no specific regulator in charge of data protection. However, state administrative authorities have an obligation to protect personal confidential information that has become available to them during the course of their operations and are prohibited from disclosing this information unless required under the law.

33.2 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.

33.3 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.

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

Not applicable.

33.5 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)?

Although there is no legal obligation to do so, it might be advisable to notify individuals in the event of a data breach, depending on the nature of the breach and of the data concerned. For instance, if the breach is of a criminal nature (Disclosure of personal confidential information, Article 136 of the Criminal Code of Mongolia), then the affected party will be notified in order for the criminal proceeding to be commenced. Similarly, in the case of credit card data breaches, the bank will notify the affected person, as the proper and timely notification of individuals may help to prevent greater damage being caused by the data breach.

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

The key legislation is the Law of Mongolia "On Personal Secrecy" dated 21 April 1995 (as amended). There is also other legislation such as the Civil Code of Mongolia (2002), Law of Mongolia on Banking (2010), and the Law of Mongolia on Organisational Confidentiality (1995) which protect personal confidential information.

33.7 Contact information for Data Protection Authority:

Not applicable.

For more information, contact:

Name: Elisabeth Ellis
Firm: MinterEllison
Address: Suite 612 Central Tower, Great Chinggis Khaan's Square 2, Sukhbaatar District – 8, Ulaanbaatar, Mongolia
Telephone: +976 7700 7780
Fax: +976 7700 7781
Email: elisabeth.ellis@minterellison.com
Website: www.minterellison.com

34. MONTENEGRO

34.1 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)?

A company that performs or is authorised to perform electronic communications activities ("operator") is required to notify individuals, the Agency for Electronic Communications and Postal Services ("EKIP") and the Personal Data Protection Agency ("DPA") of certain data breaches.

A company performing activities under the public authority or a company that learns or comes into possession, while performing its business activities, of certain state-related secret information, including secret data of foreign countries and international organisations (e.g., information classified as confidential, secret or top secret) must notify the authorised person that determined the level of data secrecy, in accordance with the law, of any security breach pertaining to such data.

There is no legal obligation to inform the affected individuals, EKIP or DPA in other cases. Still, if a data breach has elements of a criminal offence (e.g., unauthorised collection of personal data, unauthorised access to a computer or computer network, etc.), principally, every person or a regulatory body (including EKIP and DPA) is required to notify the police.

34.2 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 operator is required to notify EKIP and DPA in the case of any breach of users' personal data or privacy.

The operator is required to notify users if a data breach could be detrimental to their personal data or privacy. Exceptionally, the operator would not be required to notify users of such a data breach if it obtains approval from EKIP.

The operator is also required to notify its users of a network security risk exceeding the scope of measures that the operator is obliged to apply, and to inform them about available measures to eliminate such security risk and its consequences, including costs of implementing such measures.

The operator is required to notify EKIP of any breach of security or integrity of electronic communications networks and services that has significantly impacted the operator's activities. EKIP is authorised to inform the public about such violations reported by the operator or to request that the operator to do so if it assesses that releasing such information is in the public interest.

The entity does not have to be a data controller or a data processor for such obligations to apply.

34.3 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?

Notifications to EKIP and the DPA should contain a description of the consequences of the data breach, and proposed measures to eliminate the source of the data breach or measures that have already been taken to do so.

Notification to users should describe the data breach, the personal data breached, contact details of the operator's authorised person who can provide users with more detailed information, and the proposed measures to minimize the negative impact of the breach on users' personal data.

In practice, operators notify users via email.

Notifications to EKIP and DPA should be made in written form in accordance with the bylaws adopted by EKIP.

Notification to EKIP of a security breach resulting in interruption of services must be provided within one hour of the security breach, while a full report on the same security breach should be provided to EKIP within three work days, in the form prescribed by the bylaws.

Notification of the authorised person of any data breach in relation to confidential or secret state-related data must be performed immediately.

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

For failure to notify its users, EKIP or the DPA, a company (operator) may be fined in the range of EUR 6,000 to 30,000, while the responsible person in the company may be fined in the range of EUR 300 to 3,000.

For failure to notify the authorised person of any data breach pertaining to state-related data classified as confidential or secret, a company may be fined in the range of EUR 1,100 to 16,000, while the responsible person in the company may be fined in the range of EUR 100 to 1,100.

Failure to notify the police of a data breach that has criminal elements may result in criminal liability for both the company and the responsible person in the company.

34.5 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 if there is no legal obligation to do so, notification to individuals may be recommended in the event of a data breach, as it may mitigate or exclude the company's liability in case of any damages incurred by individuals.

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

These are:

- Personal Data Protection Law;
- Law On Electronic Communications and EKIP's bylaws;
- Law on Data Secrecy;
- Law on Protection of Undisclosed Data;
- Law on the Ratification of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data; and
- Law on the Ratification of the Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data regarding supervisory authorities and trans-border data flows.

34.7 Contact information for Data Protection Authority:

Name:	Personal Data Protection Agency
Address:	Kralja Nikole 2, 81000 Podgorica, Montenegro
Telephone:	+382 20 634 894
Fax:	+382 20 634 883
Email:	azlp@t-com.me
Website:	www.azlp.me

Name:	Agency for Electronic Communications and Postal Services (EKIP)
Address:	Bulevar Džordža Vašingtona 56, 81000 Podgorica, Montenegro
Telephone:	+382 20 406 762
Fax:	+382 20 406 702
Email:	ekip@ekip.me
Website:	www.ekip.me

For more information, contact:

Name:	Milica Popović
Firm:	CMS Montenegro
Address:	Bulevar Džordža Vašingtona 3/22, 81000 Podgorica, Montenegro
Telephone:	+382 20 416 070 / +381 11 320 8900
Fax:	+382 20 416 071
Email:	milica.popovic@cms-rrh.com
Website:	www.cms-rrh.com

35. MOZAMBIQUE

35.1 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)?

Mozambique does not have any specific laws governing data breach notifications, besides those related to the financial sector. Accordingly, under Mozambican law, there is no specific legal obligation or requirement to notify either affected individuals or any regulator (in fact, there is no Data Protection Authority in Mozambique) of a data breach.

The only legal rules that relate to privacy and data protection in Mozambique are:

- A general protection enshrined in Article 71 of the Mozambican Constitution (ideas of protection of personal data in computer records, requirements for access to databases and the use by public and private authorities of these databases or computer media);

- The Mozambican Civil Code establishes the right to privacy (v. Article 80), thus instituting the regime for the confidentiality of personal data, according to which the collection, processing and storage of personal data requires the explicit permission of the interested parties, insofar as the rights of personality can only be limited voluntarily (v. Article 81).

Regarding financial institutions, please note:

- Mozambican bank legislation that regulates the prevention of money-laundering in the financial system (Law no. 7/2002, February 5 and Decree no. 37/2004, of 8 September) provides that all banks are lawfully authorised to collect all the relevant personal data of their clients when performing some specific operations, such as opening a bank account. Moreover, banks are obliged to keep and are responsible for the personal collected data of their clients for a maximum period of 15 (fifteen) years, counted from the date of the closing of the bank accounts or performance of the bank operations.

- Notwithstanding the general principle that all personal data collected by the banks are protected by professional privilege under the provision of Article 18 of Law no. 7/2002, February 5, banks must collaborate with any judicial or criminal authorities in the event of a formal investigation by sharing all the required information (including personal data information), without any prior authorisation or consent given by the client, nor implying any contractual or civil liability of the bank.

- Specifically regarding credit or debit cards, the Notice 1/GBM/2014, of July 4, of the Central Bank of Mozambique, establishes that in the case of intentional or unintentional personal data breach, banks are explicitly obliged to carry out any notifications to their clients and for taking all necessary actions to prevent any damage from such security or integrity incidents, threats or vulnerabilities.

The above notwithstanding, requirements for access to databases and transmission of data have yet to be regulated, including the definition of what is meant by personal data, as well as the consequences of the violation of that right.

35.2 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.

35.3 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.

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

Not applicable.

35.5 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)?

Considering the above-mentioned legislative gap on data protection matters and bearing in mind that Mozambique has no Data Protection Authority, it is nearly impossible to address this matter by giving an accurate response about the standard required notification procedure to follow and the exact consequences of the violation of personal data.

Even knowing that, it is recommended, both for private or administrative entities, to formally notify the respective individuals, in the event of a data breach. From a legal point of view, and under the assumption that either the private or the administrative entity were responsible for collecting and storing the same data, such notification shall be interpreted as industrious, apart from useful for mitigating damages.

As regards credit card data breaches please refer to 35.1 above.

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

Despite not directly addressing the issue, the Constitution of Mozambique, the Mozambican Civil Code, the Labour Law (Law no. 23/2007, of August 1) and Law no. 34/2014, of 31 December, provide for certain guidelines.

On the one hand, Article 71 of the Constitution establishes that the law shall provide for (i) a general protection of personal data in computer records, (ii) requirements for access to databases and (iii) the terms of use by public and private authorities of these databases or computer media. However, these legal rules do not yet exist.

On the other hand, Article 80 of the Civil Code institutes the reserve on the intimacy of private life and Article 81 of the same law provides for the general regime of confidentiality of personal data, according to which the collection, processing and storage of personal data requires the explicit permission of the interested parties.

Regarding employment, Article 6 of the Labour Law provides for the protection of personal data, having left to specific legislation (which does not yet exist), the regulation of the use of computer files and access to personal data related with a job applicant or employee and, moreover, attributes the employee, as a general rule, the right to confidentiality of correspondence of a personal nature made by means of electronic messages.

Finally, Law no. 34/2014, of 31 December, regulates the exercise of the public right to information and public democratic participation within the procedure and interaction between private entities or individuals and administrative and governmental bodies or entities. According to the referred law, the exercise of public right to information and public democratic participation shall be made with respect to human dignity, namely, observing and respecting the right to honour, good name and reputation, as well as the right to defend the private life or data of the people concerned.

Consistent with that main principle, one of the most important rules introduced by Law no. 34/2014, of 31 December, is that personal data or information regarding the privacy of people concerned, contained either on electronic or physical files held by such public entities, are classified as confidential and cannot be shared with any third or interested parties, unless in the case of express written consent of the people concerned or in the case a court decision requires it. Please note that the breach of said terms and conditions in the use of confidential information shall be punished with fines and may lead to a criminal prosecution, on a case-by-case basis.

35.7 Contact information for Data Protection Authority:

Not applicable.

For more information, contact:

Name: Tomás Timbane
Firm: TTA Sociedade de Advogados
Address: Edifício Millennium Park, Torre A, Avenida Vladimir Lenine, nº 179, 6º Dtº, Maputo – Moçambique
Telephone: +258 843 141 820
Email: tomas.timbane@tta-advogados.com
Website: www.tta-advogados.com

Name: Miguel Spinola
Firm: PLMJ Sociedade de Advogados, RL
Address: Edifício Eurolex, Avenida da Liberdade, 224, 1250-148 Lisbon – Portugal
Telephone: +351 213 197 446 or +351 916 346 219
Fax: +351 21 319 74 00
Email: miguel.spinola@plmj.pt
Website: www.plmj.com

36. THE NETHERLANDS[25]

36.1 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)?

Article 34a of the Dutch Data Protection Act entered into force on 1 January 2016. It introduces two obligations for the data controller to – under certain conditions – report data breaches to (i) the Data Protection Authority (DPA) and (ii) the person whose data is involved (data subject). A "data breach" is defined as a breach of the technical and organisational measures required to protect data under Article 13 of the Dutch Data Protection Act (implementing Article 17(1) of EU Directive 95/46/EC).

- Notifying the DPA is mandatory if there is a breach that leads to a considerable chance of serious adverse effects for the protection of personal data.

- The notification of data subjects is mandatory if the breach may have unfavorable effects on the data subject's privacy. The data subject does not have to be notified if technical security measures have been taken to encrypt the personal data involved, or otherwise render the data incomprehensible.

In addition, there are certain sector-specific data breach notification obligations:

Telecoms: providers of publicly available electronic communications services must notify the DPA (Note: this used to be the Consumer & Markets Authority prior to 1 January, 2016) 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. This notification obligation is an implementation of Article 4, EU Directive 2002/58/EC (e-Privacy Directive).

Banking: under the Dutch Financial Supervision Act, banks and other financial enterprises must report incidents to The Netherlands Central Bank and The Netherlands Authority for the Financial Markets. A financial enterprise is exempted from reporting data breaches to data subjects – only the obligation to notify the DPA is applicable to financial enterprises (Article 34a(10) Dutch Data Protection Act).

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

36.2 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?

Types of data

The general obligation to report data breaches is deliberately not confined to certain categories of personal data or certain specific processing activities. Furthermore, the legislature emphasized that the notification obligation solely regards the breach of measures intended to protect personal data, so the "unlawful processing" as such is not a data breach.

With regard to the sector-specific notification obligations, we note the following:

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 obligation 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.

Entity to which the obligations apply

The obligation to notify the DPA and/or data subjects is on the data controller who is subject to the laws of the Netherlands – to be determined in accordance with Article 4 of the Dutch Data Protection Act. It is the data controller's responsibility to make sure that any data processor it engages implements appropriate security measures and reports any data breaches to the data controller, in order to enable the data controller to be able to comply with its notification obligation.

36.3 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?

Content of the notice

The notification to the DPA – based on both the obligations of the Dutch Data Protection Act and Dutch Telecommunications Act – shall in all cases include the following information, to the greatest possible extent:

- Nature of the data breach;
- Agencies/bodies that can provide more information on the data breach;
- Recommended measures to limit the adverse effects of the data breach;

- Description of the actual and potential effects of the data breach; and
- Measures taken or suggested to remedy such actual or potential effects.

The notification sent to data subjects shall include all information necessary to ensure proper and careful notice, which is to be assessed on a case-by-case basis depending on the nature of the breach, the consequences of the data breach for the processing of personal data, the number of data subjects affected and the costs accompanied with such notice.

Time period within which the notice must be given

The criterion used is "prompt notification". Although there is no specific maximum time period, the DPA mentions a 72-hour notice period in their policy guidelines.

Method of giving notice

No specific method is required. Notice to the DPA may be given by filling out a designated form which is available on the DPA's website. Notice to data subjects may be given in any form appropriate given the circumstances (e.g., individual notices in case of a small number of affected data subjects or notice by mass media in the event of a large number of affected data subjects).

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

- Violation of the notification obligations under the Dutch Telecommunications Act: a fine of up to EUR 450,000 could be imposed.
- Violation of article 34a of the Dutch Data Protection Act: a fine of up to EUR 820,000 may be imposed by the DPA, depending on the exact violation. In the event of willful misconduct or gross negligence, fines may be imposed directly, without prior warning. In other situations, the DPA will be required to issue a binding instruction prior to actually imposing the fine. The fine also applies to a violation of the general obligation to cooperate with the instructions of a public administrative body (like the DPA) under Article 5:20 of the Dutch General Administrative Law Act.

36.5 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)?

Whether notification of 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 consult external advisers and/or the competent regulatory authority (DPA or sector-specific authority) in such cases prior to notification.

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

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

- Dutch Data Protection Act;
- Dutch Telecommunications Act; and
- Data Breach Policy Guidelines 2015 (issued by the Dutch Data Protection Authority).

36.7 Contact information for Data Protection Authority:

Name:	Data Protection Authority (*Autoriteit Persoonsgegevens*)
Address:	Juliana van Stolberglaan 4-10, 2595 CL Den Haag (The Hague)
Telephone:	+31 70 888 8 00
Fax:	+31 70 888 8501
Website:	www.autoriteitpersoonsgegevens.nl

For more information, contact:

Name:	Hendrik Struik
Firm:	CMS Netherlands
Address:	Newtonlaan 203, 3584 BH Utrecht, The Netherlands
Telephone:	+31 30 212 1726
Fax:	+31 30 212 1157
Email:	hendrik.struik@cms-dsb.com
Website:	www.cms-dsb.com

37. NEW ZEALAND

37.1 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 New Zealand law to notify either affected individuals or the DPA (the Office of the Privacy Commissioner).

Note that New Zealand privacy law is due to undergo significant reforms in the near future. No legislation has yet been introduced to Parliament as of the end of 2015. Law Commission reports and other related commentary suggest that some degree of mandatory breach notification will be introduced as part of the reforms, although the nature and extent of such obligations is, as yet, unknown.

37.2 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.

37.3 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.

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

Not applicable.

37.5 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 DPA has issued voluntary guidelines with key steps for agencies that become aware of a data breach originating from their organisation. The possibility of notification is noted as one of the key steps to be considered.

The DPA recommends that affected individuals be notified if notification is likely to mitigate the damage arising from the breach, and lists several factors to be considered in this assessment. The DPA notes that each incident needs to be considered on a case-by-case basis to determine whether privacy breach notification is necessary.

Agencies are also encouraged to inform the DPA of material privacy breaches so that it is aware of the breach and can effectively handle any complaints or inquiries (but note that this is not a legal requirement).

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

The key legislation is the Privacy Act 1993, which contains 12 Information Privacy Principles.

Under the Privacy Act sit six Information Privacy Codes that apply the Information Privacy Principles in specific sectors (e.g., health, credit reporting and telecommunications).

The Crimes Act 1961 contains several provisions for criminal breach of privacy, relating primarily to unlawful interception of communications and intimate visual recordings.

37.7 Contact information for Data Protection Authority:

Name:	Office of the Privacy Commissioner
Address:	PO Box 10-094, The Terrace, Wellington 6143, New Zealand
Phone:	+64 0800 803 909
Email:	enquiries@privacy.org.nz
Website:	www.privacy.org.nz

For more information, contact:

Name:	Richard Wells
Firm:	Minter Ellison Rudd Watts Lawyers
Address:	Lumley Centre, 88 Shortland Street, Auckland 1010, New Zealand
Telephone:	+64 9 353 9908
Fax:	+64 9 353 9701
Email:	richard.wells@minterellison.co.nz
Website:	www.minterellison.co.nz

38. NICARAGUA

38.1 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 current Nicaraguan law, there is no legal obligation to notify either a regulator or the affected individual when a data breach occurs. The only exception to this is set by Law No. 787, Data Protection Law (hereinafter the "Law"), which establishes that when the data breach affects the information of a member of the National Police or the military, the institutions must be notified urgently by the party responsible for the data file.

While this Law does not require data breach notifications, it does protect users by establishing minimum security measures to assure the integrity, confidentiality and security of personal data to avoid its adulteration, loss, query, treatment, revelation, transfer or unauthorized disclosure. The measures shall allow the detection of deviations, intentionally or not, of private information, whether the risks come from human actions or technical means.

In the Regulation of the Law, it is established that the responsible party for the data files shall develop and implement technical and organisational security measures to assure the integrity, confidentiality and security of the personal data treated. These measures shall be in proportion to its operations, to the associated risks and to the size of the data files managed.

While Law No. 787 enables the creation of a regulator or DPA, the institution has not been created yet, which sets some barriers in the regulation and standardizing of data file security measures.

38.2 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.

38.3 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.

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

Not applicable.

38.5 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)?

Every case should be analysed independently to decide whether or not a notification of a data breach may be advisable. The security measures established by Law No. 787 enforce the right of

the affected individual to request, rectify, amend, delete, update, or cancel his/her personal data. Moreover, many factors must be taken into consideration, especially assessing the magnitude of harm that could arise from the data breach and whether the information breached may or may not be considered "sensitive data information" protected under Nicaraguan law. In such cases, the affected individual will have a chance to exert different procedures in the acquiring and protection of such information. Moreover, if the data breach was a product of negligent handling of private information, there could be some consequences in specific cases.

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

Data protection laws or guidelines that are applicable in Nicaragua are:

- Article 26 of the Political Constitution of the Republic of Nicaragua through which personal data protection is regarded as a fundamental right.
- Law No. 621 (Access to Public Information Law) and its Regulatory Decree No. 81-2007, which regulates the information handled by the Public Administration and the procedures available to affected parties to acquire, modify, or remove the information handled by public institutions or information that has been wrongfully published. Moreover, each governmental institution must create an area where the personal information (whether public or private) is stored to be more easily handled and controlled.
- Law No. 561 (General Law of Banks), which regulates the information handled by banking institutions considered confidential and sets the obligation for such information to pass through filters of risk analyzing companies accredited by the bank intendancy agency ("SIBOIF").
- Law No. 831 (Amendment to Law No. 49) regulates the Habeas Data.
- Law No. 787 (Personal Data Protection Law) and its Regulation, which regulates the procedures for personal data storage, handling, and sets security measures. Moreover, it enables the creation of a DPA or regulator, which has not yet been fulfilled.

38.7 Contact information for Data Protection Authority:

Not applicable.

For more information, contact:

Name: Angélica Argüello
Firm: Arias & Muñoz
Address: Pista Jean Paul Genie, Edificio Escala, 3er piso, Managua, Nicaragua
Telephone: +505 2298 1360
Email: angelica.arguello@ariaslaw.com
Website: www.ariaslaw.com

39. NORWAY

39.1 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.

Specific breach notification requirements apply to providers of public electronic communications services (telecommunications providers and internet service providers).

39.2 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 unauthorised distribution of personal data that should be treated confidentially.

39.3 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.

39.4 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 of 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.

39.5 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.

39.6 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.

39.7 Contact information for Data Protection Authority:

Name:	The Norwegian Data Protection Authority
Address:	P.O. Box 8177 Dep, N0034, Oslo, Norway
Telephone:	+47 22 39 6900
Fax:	+47 22 42 2350
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 23 01 1529
Fax:	+47 22 83 1712
Email:	hama@schjodt.no
Website:	www.schjodt.no

40. PANAMA

40.1 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 Panamanian law to notify either affected individuals or a regulator, such as a Data Protection Authority, of a data breach.

The National Authority for Government Innovation proposed legislation on the Protection of Personal Data; however, to date it has not been approved.

40.2 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.

40.3 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.

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

Not applicable.

Currently, there are sanctions, such as fines/penalties, in the event that a public servant refuses access to public information. Similarly, non-compliance with data protection regulations could create civil or criminal responsibility.

40.5 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 severity of the case, such as in credit card data breaches, it is advisable to notify affected customers, since there could be civil and/or criminal responsibility.

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

Panama's data protection laws and regulations are:

- The Constitution of Panama (Articles 42 to 44);
- Law 6 of January 2002, "which dictates norms for transparency in public administration, establishes Habeas Data and dictates other dispositions";

- Executive Decree 124 of May 2002, "that regulates Law 6 of January 2002";
- Law 24 of May 2002, "Whereby the service of providing information on consumer and customer credit records is regulated";
- Resolution No. JD -101 of August 1997, "Whereby the rights and obligations of users of the public services of water, sewer, electricity and telecommunications are regulated" (Article 18, establishes the right of users to the confidentiality of their information);
- Law 51 of September 2009, "For the conservation, protection and the provision of data of users of telecommunications services and dictates other dispositions";
- Law 51 of July 2008, as amended by Law 82 of November 2012 and Executive Decree No. 40 of May 2009, (Electronic Commerce Legislation) which regulate the creation, utilization and storage of electronic documents and signatures in Panama, through a registration process and the supervision of providers of data storage services; and
- Criminal Code: Rip-off/deceive and other frauds; disclosure of trade secrets; crimes against the security of electronic data.

40.7 Contact information for Data Protection Authority:

For Electronic Commerce:

Name:	The General Directorate of Electronic Commerce (Dirección General de Comercio Electrónico)
Address:	Plaza Edison, El Paical, Floors 2 & 3, Panama City, Panama
Telephone:	+507 560 0600 or +507 560 0700
Fax:	+507 261 1942
Email:	contactenos@mici.gob.pa
Website:	www.mici.gob.pa/base.php?hoja=homepage

For more information, contact:

Name:	Siaska S.S.S. Lorenzo
Firm:	Arias & Muñoz
Address:	Torre Global, Piso 24, Oficina 2401, Calle 50, Panama City, Panama
Telephone:	+507 282 1400
Fax:	+507 282 1435
Email:	siaska.lorenzo@ariaslaw.com
Website:	www.ariaslaw.com

41. PERU

41.1 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.

41.2 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.

41.3 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.

41.4 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.

41.5 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 provider under Peruvian consumer protection laws.

41.6 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).

41.7 Contact information for Data Protection Authority:

Name:	Autoridad Nacional de Protección de Datos Personales
Address:	Calle Scipion Llona No 350, Miraflores, Lima 18, Peru
Telephone:	+511 204 8020 ext. 1030
Email:	apdp@minjus.gob.pe
Website:	www.minjus.gob.pe/proteccion-de-datos-personales

For more information, contact:

Name:	Carlos A. Patron or Giancarlo Baella
Firm:	Payet Rey Cauvi Perez Abogados
Address:	Av. Victor Andres Belaunde 147, Centro Empresarial Real, Torre Real Tres Piso 12, San Isidro, Lima 27, Peru
Telephone:	+511 612 3202
Fax:	+511 222 1573
Email:	cap@prc.com.pe or gbp@prc.com.pe
Website:	www.prc.com.pe

42. PHILIPPINES

42.1 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 in exceptional circumstances as detailed in the answer to Question 42.2 below.

The National Privacy Commission has been established recently. However, the answer to Question 42.2 below sets out how notification should be made.

42.2 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 Privacy 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 disposition 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, licences 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.

42.3 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 should include 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 written notification.

42.4 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 PHP 500,000 but not more than PHP one million.

42.5 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 is processed; and
- The entity has a link with the Philippines, such as when:

(i) A contract is entered into in the Philippines, or

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

(iii) An entity 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:

i) The entity carries on business in the Philippines, or

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

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

The key pieces of legislation are:

- Republic Act No. 10173 (Data Privacy Act of 2012), on personal information;
- Republic Act No. 8792 (Electronic Commerce Act of 2000) on data message and electronic documents; and
- Special laws such as Republic Act No. 10175 (Cybercrime Prevention Act of 2012) on computer data, 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.

42.7 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 is still being organized.

For more information, contact:

Name:	Rolando V. Medalla, Jr. or Hiyasmin H. Lapitan
Firm:	SyCip Salazar Hernandez & Gatmaitan
Address:	SyCipLaw Center, 105 Paseo de Roxas, Makati City 1226, The Philippines
Telephone:	+63 2 9823 500 or +63 2 9823 600, or +63 2 9823 700
Fax:	+63 2 8173 145 or +63 2 8173 896
Email:	rvmedalla@syciplaw.com or hhlapitan@syciplaw.com
Website:	www.syciplaw.com

43. POLAND[26]

43.1 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)?

The provisions of the Act on Personal Data Protection ("PDP") do not oblige data controllers to notify relevant data subjects or the DPA of any personal data security breaches. There are no clear rules or standard practice on what actions should be undertaken in the case of a personal data security breach. In such cases however, the data controller should assess the risks posed to the parties involved on a case-by-case basis. Considering the negative consequences of the personal data security breaches for both the controllers and data subjects, the controllers may follow the recommendations presented in Opinion 3/2014 of Art. 29 of the Data Protection Working Party on personal data breach notification adopted on 25 March 2014. Pursuant to this opinion, whenever the controller has doubts regarding the likelihood of adverse effects on the personal data privacy of the data subjects, it should err on the side of caution and proceed with the notification.

There are specific regulations on personal data security breaches in the telecommunications sector. The providers of the publicly available telecommunication services are required by the Telecommunications Law to notify the DPA of every personal data security breach. If such breach is likely to adversely affect an individual subscriber or end users, the provider of the publicly available telecommunication services should also notify those individuals.

43.2 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 Telecommunications Law, a proper notification covers all personal data security breaches, e.g. destruction by accident or as a result of an illegal act, loss, change, unauthorised disclosure or access to personal data processed by the provider of the publicly available telecommunication services. Notwithstanding the obligation towards the DPA, an individual subscriber or end user must be notified if the data breach may adversely affect them, e.g., causes an unauthorised use of personal data, material damage, violation of personal rights, disclosure of bank secrecy or another professional secrecy protected by law. Notifying a subscriber or end user is not required if the provider of the publicly available telecommunication services implemented technical and organisational security measures envisaged in the PDP and its executive regulations, which make it impossible for unauthorised persons to read the data (such as encryption tools) and applied these measures to the data in question.

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

43.3 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 telecommunication services should notify the DPA of each case of personal data breach without delay but not later than three days from the detection of such breach. The same time limit applies to notifications towards subscribers or end users. The form of the notification is not specified. For evidencing purposes, the notification should be made in writing (e.g., regular mail, e-mail) and should be directed to each individual. The notification must include: the description of the personal data breach; the provider's contact details; information about recommended measures to be taken in order to mitigate the negative consequences of the breach; information about measures already undertaken by the provider; an informative description of the implication of the personal data breach; and the remedies proposed by the provider.

Additionally, a notification to the DPA should contain an indication of the assumed risk connected with the data breach and should specify whether subscribers or end users were notified. If subscribers or end users may be adversely affected by the data breach, the DPA is entitled to impose a duty to submit such a notification on a provider.

The provider is obliged to maintain a register of data breaches consisting of information about personal data infringements. The provider is obliged to enable access to the register for the DPA, subscribers, and end users. On the basis of a written outsourcing agreement, another undertaking might manage the register but the provider remains responsible for it and its content.

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

Pursuant to the Telecommunications Law, the provider of publicly available telecommunication services is subject to financial penalties for the violation of the information duties towards end users. Duties include notifications about data breaches. In the case of non-performance, the President of the Office of Electronic Communications ("OEC") may impose a financial penalty on the provider. The amount cannot exceed 3% of the revenue generated in the financial year prior to that in which the penalty is imposed. Irrespective of the above financial sanctions, the President of the OEC may impose additional fines on persons in charge of the provider, in particular a person performing managerial functions or a member of that provider's management body. The amount of the fine cannot exceed 300% of their monthly remuneration, calculated in accordance with rules regarding refunds for unused paid holidays.

The PDP does not oblige data controllers to notify the DPA of any personal data security breaches or data leaks. Nevertheless, it obliges the controller to implement safeguards to protect personal data against unauthorised disclosure. The PDP does not specify financial sanctions for non-compliance with the requirements for implementing safeguards on personal data processing in the case of a breach or non-performance of obligations specified in the Telecommunications Law. If such requirements are not satisfied however, the DPA may conduct an inspection

and issue a decision ordering the data controller to remove instances of non-compliance. As regards a data security breach in the telecommunications sector, under the provisions of the Telecommunications Law, the DPA is also entitled to issue administrative decisions that impose an obligation on the provider of publicly available telecommunication services to notify a given data subject about a personal data breach. If the provider did not establish a proper register of data breaches or manages the register in violation of relevant provisions, the DPA is entitled to issue an administrative decision ordering the provider to amend the register so as to be in compliance with the law, e.g., by remedying indicated failures.

Only in the case of the non-performance of the decision, under the general provisions on administrative enforcement proceedings, may the DPA impose enforcement fines up to approx. EUR 12,000 per instance of non-compliance. In the case of repeated fines, the lump sum cannot exceed approx. EUR 50,000.

As stated above, the notification obligation has been imposed on the providers of publicly available telecommunication services (data controllers). If the data controller entrusted the processing of personal data to the data processor and the data security breach took place within the data processor's organisation, the data controller is still responsible for personal data security and it performs the notification obligation.

43.5 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 may be cases when notification about data braches towards the data subjects is recommended. Individual notification policies should be shaped with respect to the safety, financial situation, and personal interests of data subjects, which entails notifying the subjects about leaks of personal data concerning bank or credit accounts, IDs, e-mail passwords, and sensitive data. In some instances, it might be recommended to undertake actions mitigating possible negative consequences of a given data leak in order to prevent relevant data subjects from seeking damages. Whenever a data controller suspects that personal data security has been compromised by a third party, the controller should consider notifying the relevant investigative authorities (including the prosecution service) about a suspected offence having been committed. The above-mentioned Opinion 3/2014 may prove helpful for data controllers. It contains a non-exhaustive list of examples where data subjects should be notified. It also indicates instances when such notification can be omitted but, nevertheless, it suggests notifying data subjects of such breaches to demonstrate due care, even at the cost of overly excessive prevention.

Every case of data breach should be examined on an individual basis and assessed according to the three security criteria: (i) availability of the breach corresponding to the accidental or unlawful destruction or loss of data; (ii) integrity of the breach corresponding to the alteration of data; and (iii) confidentiality of the breach corresponding to an unauthorised disclosure

of, or access to personal data. Additionally, when the data controller is unable to identify all individuals adversely affected by a given breach, they can notify relevant individuals through advertisements in the national media or request support from other providers or controllers in possession of contact details. For example, the provider might request assistance from intermediary payment agents when the details of cardholders are lost. Data controllers may also collaborate with competent public authorities, having reported to them that notifying all affected individuals is impossible.

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

The key legislation is the Act on Personal Data Protection of 29 August 1997 (consolidated ver.: Journal of Laws of 2014, item 1182 as amended) and the Act of 16 July 2004 Telecommunications Law (consolidated ver.: Journal of Laws of 2014, item 243 as amended).

Directive 95/46/EC of the European Parliament and of the Council 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 has been implemented into Polish law.

43.7 Contact information for Data Protection Authority:

Name:	The Bureau of the Inspector General for Personal Data Protection (Biuro Generalnego Inspektora Ochrony Danych Osobowych)
Address:	ul. Stawki 2, 00-193 Warszawa, Poland
Telephone:	+48 22 8607 086
Fax:	+48 22 8607 086
Email:	kancelaria@giodo.gov.pl
Website:	www.giodo.gov.pl

For more information, contact:

Name:	Agata Szeliga or Katarzyna Paziewska
Firm:	Sołtysiński Kawecki & Szlęzak
Address:	ul. Jasna 26, 00-054 Warszawa, Poland
Telephone:	+48 22 608 7006 or +48 22 608 7190
Fax:	+48 22 608 7070
Email:	agata.szeliga@skslegal.pl or katarzyna.paziewska@skslegal.pl
Website:	www.skslegal.pl

44. PORTUGAL[27]

44.1 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 communications 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 results in the risk of identity fraud, physical injuries, humiliation, or 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 in case of a personal data breach.

44.2 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.

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

44.3 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.

44.4 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 offence punishable with a fine ranging from a minimum of EUR 500 to a maximum of EUR 20,000 when the defaulter is an individual, and from a minimum of EUR 2,500 to EUR 2,500,000 when a legal entity 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 EUR 50 and EUR 100,000.

44.5 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.

44.6 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).

44.7 Contact information for Data Protection Authority:

Name:	Comissão Nacional de Protecção de Dados (CNPD)
Address:	Rua de São Bento, 148 3º, 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

45. RUSSIA

45.1 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 formal legal obligation to notify. However, the personal data operator is required to immediately take the necessary measures in order to remedy the effects of a data breach. If the operator (data controller) fails to remedy the breach connected with the non-authorised processing of personal data within the stipulated term, or the data have been destroyed in course of such remedy, notification of the data subject is required.

In the meantime, there is a fairly recent initiative to introduce a mandatory notification of the DPA in case of a data breach. Still, as of today, it is unclear when and in what form this legislation is going to be enacted, if at all.

45.2 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 those minor cases when rectification of the breach did not succeed, notification is required. It is an obligation of the operator (data controller) to notify the data subject.

45.3 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 specified.

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

No specific liability for failure to notify or general liability for breach of personal data processing rules are applicable.

45.5 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 as 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 affected individuals may help to prevent greater damage caused by a data breach.

Further, the data subjects are entitled to access their personal data, undertake various measures to protect their rights and send the corresponding requests to the data processor.

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

The key legal act in the area is the Federal Law No. 152-FZ dated 27 July 2006, On Personal Data.

45.7 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 49 5987 6800
Fax:	+7 49 5987 6801
Email:	rsoc_in@rkn.gov.ru
Website:	http://rkn.gov.ru/

For more information, contact:

Name:	Maxim Boulba
Firm:	CMS Russia
Address:	Gogolevsky Blvd. 11, 119019 Moscow, Russia
Telephone:	+7 49 5786 4000
Fax:	+7 49 5786 4001
Email:	maxim.boulba@cmslegal.ru
Website:	www.cmslegal.ru

46. SERBIA

46.1 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)?

A company using an information-communication system ("ICS") as a part of its business activities ("ICS operator") may be required to notify the competent authority in the event of an incident that may significantly affect data security of the ICS.

The principal competent authority for ICS data breach notification is the Ministry of Trade, Tourism and Telecommunications, but depending on the type of the business activity and ICS, the company may be required to instead notify other regulatory authorities.

For example, a company that performs or is authorised to perform electronic communications activities ("EC operator") is required to notify the Regulatory Agency for Electronic Communications and Postal Services ("RATEL") of any such incident significantly affecting data security of the electronic communication network. The EC operator is also required to notify the affected individuals in the event of certain types of data breaches.

On the other hand, banks and financial payment institutions are required to notify the National Bank of Serbia ("NBS") of any such incident that may have significant impact on data security. They are also required to notify NBS of certain data breaches (e.g., credit card fraud, skimming, unauthorised use of clients' data, etc.) as a part of standard reports submitted periodically to NBS.

There is no legal obligation to inform the Ministry of Trade, Tourism and Telecommunications, affected individuals, RATEL, NBS or the Serbian Data Protection Authority ("DPA") in other cases. However, if personal data was breached, the relevant competent authority will also notify the Commissioner for Information of Public Importance and Personal Data Protection, who is authorised to start a separate investigation and, if necessary, take certain corrective measures towards the data operator.

If a data breach has elements of a criminal offence (e.g., unauthorised collection of personal data, unauthorised access to a computer or computer network, etc.), the ICS operator is required to notify the police, while the relevant competent authority is also required to further notify the Ministry of Internal Affairs and the District Attorney's Office.

In case of certain ICS security risks or incidents, which have a tendency to become high risk or may impact other countries, upon notification from the ICS operator the relevant competent authority may inform the relevant data protection or law enforcement authority in other affected countries in accordance with the ratified international treaties.

Therefore, if a company operates a transnational ICS or an ICS with a cross-border element, it is prudent that the ICS operator checks whether laws of the affected country require notification of that country's competent authority and, if this is the case, proceed to independently notify that authority in the affected country prior to any notification issued by the Serbian competent authority.

46.2 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?

Principally, the ICS operator is required to notify the relevant competent authority of any incident that may significantly affect data security of the ICS, where the incident is defined as an external or internal event or circumstance that endangers or affects the data security of the ICS.

Also, if there is a risk of breach of security or integrity of a public electronic communications network and services, such as unauthorised access, significant loss of data, violation of the communication secrecy or security of personal data, etc., the EC operator is required to notify its users or subscribers of such a risk.

If such a risk falls outside of the scope of the measures that the EC operator is obliged to apply, the EC operator is required to inform its users or subscribers about possible protection measures and costs related to implementation of such measures.

In particular, the EC operator is required to notify RATEL of any breach of security or integrity of public electronic communications networks and services that has significantly impacted the EC operator's activities, and especially to notify of any breaches or violation pertaining to personal data protection or user/subscriber privacy.

RATEL is authorised to inform the public about such violations reported by the EC operator or request the EC operator to do so, if it assesses that releasing such information is in the public interest. Also, under the same conditions, other relevant competent authorities are authorised to notify the public of ICS data breaches reported by the ICS operators.

The entity does not have to be a data controller or data processor for such obligations to apply.

The ICS data breach notification requirement applies to any company, public entity or public authority that uses ICS to perform a public duty or exercise a public authority, stores or processes personal data considered especially sensitive, or performs business activities in the sectors of (1) production, transport and distribution of electric energy, (2) coal production and processing, (3) research, production, processing, transport and distribution of oil and natural or liquid gas, (4) sale of oil and oil derivatives, (5) rail, postal and air transport, (6) electronic communications, (7) financial institutions, (8) communal activities, (9) waste management, (10) health care.

46.3 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, there is no prescribed method or time for notification or content of notice, except for standard reporting to NBS, which is regulated by NBS's bylaws. It is expected that the method and content of notification in the event of an ICS data breach will be regulated in the future by separate bylaws.

In practice, EC operators notify users and subscribers via email.

The notifications to RATEL are usually given by email and registered mail. Until explicit regulations exist, we recommend that all ICS operators apply the same method when notifying the relevant competent body.

In case of a serious data breach, a breach pertaining to national security or data classified as secret, beside notifying RATEL, EC operators should also notify the Security Information Agency. Although, not explicitly regulated, such a notification by an ICS operator would be also prudent in cases of any ICS data breaches.

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

For failure to notify the relevant competent authority of the ICS data breach, the company (ICS operator) may be fined in the range of EUR 410 to 4,070, while the responsible person in the company may be fined in the range of EUR 40 to 410.

For failure to notify RATEL, the company (EC operator) may be fined in the range of EUR 4,070 to 16,260, while the responsible person in the company may be fined in the range of EUR 410 to 1,220. In addition, both the company and the responsible person may be punished by prohibition from performing certain business activities for up to three years.

If the NBS as a regulatory body learns of any significant data breaches that may concern the lawful business operations and practices of a bank or a financial payment institution, it may take certain corrective measures towards such entities as prescribed by the Law on Banks.

Failure to notify the relevant competent authority or the police of a data breach that has criminal elements may result in criminal liability for both the company and the responsible person in the company.

46.5 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)?

Even if there is no legal obligation to do so, notification to individuals may be recommended in the event of a data breach, as it may mitigate or exclude the company's liability in case of any damages incurred by individuals.

46.6 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);
- 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);
- Law On Electronic Communications ("Official gazette of RS", Nos. 44/2010, 60/2013 and 62/2014);

- Law on Information Security ("Official gazette of RS", No.6/2016);
- Law on Banks ("Official gazette of RS", Nos. 107/2005, 91/2010 and 14/2015) and bylaws of the National bank of Serbia;
- Law on Protection of Business Secrecy ("Official gazette of RS", No. 72/2011); and
- Law on Data Secrecy ("Official gazette of RS", No. 04/2009).

46.7 Contact information for Data Protection Authority:

Name:	The Commissioner for Information of Public Importance and Personal Data Protection
Address:	Bulevar kralja Aleksandra 15, 11000 Belgrade, Serbia
Telephone:	+381 11 340 8900
Fax:	+381 11 334 3379
Email:	office@poverenik.rs
Website:	www.poverenik.rs

Name:	Regulatory Agency for Electronic Communications and Postal Services (RATEL)
Address:	Višnjiĕva 8, 11000 Belgrade, Serbia
Telephone:	+381 11 324 2673
Fax:	+381 11 324 2673
Email:	ratel@ratel.rs
Website:	http://www.ratel.rs

Name:	Ministry of Trade, Tourism and Telecommunications of the Republic of Serbia
Address:	Nemanjina 22-26, 11000 Belgrade, Serbia
Telephone:	+381 11 361 6536
Fax:	+381 11 361 0297
Email:	telekomunikacije@mtt.gov.rs
Website:	http://mtt.gov.rs/

For more information, contact:

Name:	Ksenija Ivetić or Radivoje Petrikić
Firm:	Petrikić & Partneri AOD in cooperation with CMS Austria
Address:	Cincar Jankova 3, 11000 Belgrade, 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

47. SINGAPORE

47.1 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 specific legal obligations or requirements under Singapore law to notify the affected individuals or the data protection authority (i.e., Personal Data Protection Commission) in the event of a data breach. However, the Personal Data Protection Commission ("PDPC") published a Guide to Managing Data Breaches ("Guide") on 8 May 2015. Although the Guide is not legally binding, it provides guidance on how an organisation should manage and respond to data breaches.

According to the Guide, as a matter of good practice, organisations should notify the following persons upon discovery of a data breach:

- Any individuals who are affected by the data breach;
- Any interested third parties (such as banks, credit card companies, Monetary Authority of Singapore, Infocomm Development Authority, the Singapore Police Force, etc.); and
- The PDPC, especially if sensitive information was disclosed as a result of the data breach.

47.2 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 Guide applies to all organisations, regardless of whether it is a data controller or data processor. The Guide also defines a data breach as an "unauthorised access and retrieval of information that may include corporate and personal data". The Personal Data Protection Act 2012 defines personal data as any data by which the individual can be identified. Examples of personal data are name and contact details.

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

Informing the affected individual

The Guide advises all organisations to notify the affected individuals immediately if their sensitive personal data is disclosed as a result of a data breach, and notify the affected individuals once the data breach is resolved.

In notifying the affected individual of such data breaches, the Guide states that the organisation should provide the affected individual with the following information:

- How and when the data breach occurred;

- Types of personal data affected by the data breach;
- What rectification measures will be implemented by the organisation;
- Clear instructions on what the affected individuals can do to protect themselves; and
- How the organisation can be contracted if the affected individual requires further information or assistance.

Due to the urgency of the situation and the large number of individuals affected by a data breach, there is no fixed method of giving notice as the organisation should adopt the most effective ways to contact the affected individuals.

Informing the PDPC

When notifying the PDPC of such data breaches, the organisation should provide the following information to the PDPC:

(i) The extent of the data breach occurs;

(ii) The number of personal data affected by the data breach;

(iii) How the data breach occurred;

(iv) Whether the data breach has been rectified;

(v) At the time of the data breach, what measures and processes that the organisation had implemented to guard against data breach;

(vi) Whether the individuals affected by the data breach were notified;

(vii) If the answer to (vi) is no, the organisation must inform PDPC on when it intends to inform these affected individuals; and

(viii) Contact details of the organisation's representative.

Organisations are strongly encouraged to report all instances of data breach as soon as possible to the PDPC.

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

Currently, there are no penalties or fines imposed on an organisation for its failure to notify. However, the Guide states that an organisation's failure to notify will affect the PDPC's decision on whether an organisation has reasonably protected personal data under its control or possession. Under section 29(2)(d) of the Personal Data Protection Act 2012, the PDPC is entitled to impose a fine of up to SGD one million in the event of a data breach if the PDPC is of the view that the organisation failed to protect the personal data under its control or in its possession.

Further, an individual affected by the data breach may bring a civil claim against the organisation for its failure to protect the personal data under its control or in its possession. If the individual is successful, the court may award damages or any other relief that it deems fit.

47.5 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 credit card breaches)

Although there are no legal obligations, the Guide recommends that organisations should notify the individuals who are affected by a data breach.

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

The Personal Data Protection Act 2012 came into force on 2 July 2014. This is the main data protection law in Singapore and it governs the collection, use, disclosure and protection of personal data.

The PDPC, which enforces the Personal Data Protection Act 2012, has issued numerous guidelines since its inception to provide guidance on how the Personal Data Protection Act 2012 will be interpreted and enforced. For instance, the guidelines issued by PDPC include the Advisory Guidelines on Key Concepts in the PDPA, Guide to Managing Data Breaches and sectoral advisory guidelines to address persona data issues that are sector-specific.

In addition, sectoral codes and guidelines such as the Technology Risk Management Guidelines, issued by the Monetary Authority of Singapore, provide guidance on how financial institutions can adopt sound practices and processes for managing technology and preventing data loss.

47.7 Contact Information for Data Protection Authority

Name:	Personal Data Protection Commission
Address:	460 Alexandra Road, #10-02 PSA Building, Singapore 119963
Telephone:	+65 6377 3131 (for General Enquiries) or +65 6508 7333 (Personal Data Protection Commission)
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 6885 3638
Fax:	+65 6225 1838
Email:	gilbert.leong@rodyk.com
Website:	www.rodyk.com

48. SLOVAKIA[28]

48.1 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 obligation in Slovakia to notify affected individuals or a regulator such as a DPA. According to the Act No. 122/2013 Coll. on Personal Data Protection (as amended by the Act No. 84/2014), a personal data officer has to notify the controller in writing, without undue delay, of any breach of statutory provisions of the Act. Current legislation focuses more on prevention of the breach. However, the proposed EC Regulation on Protection of Personal Data introduces a general notification obligation, based on the concept of notification of personal data breaches pursuant to Article 4, subsection 3 of the Directive on Privacy and Electronic Communications 2002/58/EC. Thus, it is expected that the general notification obligation in Slovakia will be subject to changes in the upcoming months.

In a case of data breach in the electronic communication sector, an enterprise that provides public services shall be obliged to notify the Regulatory Authority for Electronic Communications and Postal Services (not the DPA) and the subscribers about the breach if conditions under the Act no. 351/2011 Coll. on electronic communications were fulfilled.

In the sector of critical infrastructure providers, the principle of cybersecurity was recently addressed by the Slovak Government and a concept paper on cybersecurity was released for intergovernmental comments. It is expected that an Act on cybersecurity will be proposed, including notification obligations for critical infrastructure providers.

Opinion No. 03/2014 of the Data Protection Working party[29] also works as a guidance to the controllers in a case of personal data breach and it proposes a non-exhaustive list of examples where the data subject shall be notified. According to this opinion, notifications to data subjects should be made without undue delay and shall not be dependent on the notification of the personal data breach to the competent national authority.

48.2 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 a case of a data breach in the electronic communication sector, every breach shall be notified to the Regulatory Authority for Electronic Communications and Postal Services according to the Act no. 351/2011 Coll. on electronic communications. Subscribers shall be notified only on data breaches that may adversely affect their personal data or privacy. Notification is not required if the enterprise demonstrated to the Telecommunications Office that it has implemented

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

[29] Working party set up under Article 29 of Directive 95/46/EC.

appropriate technological protection measures and that those measures were applied to the data concerned by the security breach.

Mandatory notification of breach applies to enterprises that provide public services, regardless of whether they act as a data controller or data processor. Where another provider is contracted to deliver part of the electronic communications service without having a direct contractual relationship with subscribers, this other provider shall immediately inform the contracting provider in the case of a personal data breach.

48.3 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 to the Regulatory Authority for Electronic Communications and Postal Services shall contain:

- A description of the nature of the personal data breach;
- Effects of the personal data breach;
- Measures proposed or carried out by the undertaking to mitigate the adverse effects of the personal data breach;
- Date of the personal data breach; and
- Date of the discovery of the personal data breach by the undertaking.

Notification to the subscribers and users concerned about the personal data breach shall contain:

- Description and manner of the personal data breach;
- Contact points where more information can be obtained; and
- Measures recommended to mitigate adverse effects of the personal data breach.

Notifications must be given without undue delay. In line with the Regulation No. 611/2013/EC on measures applicable to notification of personal data breaches, the Methodical Instruction of the Regulatory Authority for Electronic Communications and Postal Services for the notification of the personal data breach prescribes a 24-hour notification period.

As soon as possible but no later than three days after the first notification, the provider shall give a second notification to the Regulatory Authority. This second notification shall contain:

- A summary of the incident that caused the personal data breach (including the physical location of the breach and of the storage media involved);

- The number of subscribers or individuals concerned;
- Potential consequences and potential adverse effects on subscribers or individuals; and
- Technical and organisational measures, taken by the provider to mitigate potential adverse effects.

Notification shall be sent as a completed form via e-mail to the address oou@teleoff.gov.sk by a person responsible for enterprise security and integrity of networks and services. The form must be completed following the instructions and sent by mail or email. Further details are available at www.ezd.sk/ipb/oou/legislativasr.php.

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

The Regulatory Authority for Electronic Communications and Postal Services shall impose a sanction up to EUR 300,000 on the enterprise that failed to fulfill its notification obligation in case of a data breach, according to the Act no. 351/2011 Coll. on electronic communications.

48.5 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 a notification of such breach.

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

The main data protection laws and guidelines are:

- Act. No. 122/2013 Coll. on Personal Data Protection;
- Act. No. 117/2013 Coll. on the scope of security measures in the area of personal data protection;
- Act. No. 164/2014 Coll. on details of exams for individuals to perform the function of the data protection officer;
- Act. No. 165/2014 Coll. on the scope and documentation of security measures;
- Act No. 351/2011 Coll. on electronic communications;
- Opinion No. 03/2014 of the EC Article 29 Working Party;
- Directive on privacy and electronic communications 2002/58/EC;
- Regulation No. 611/2013/ EC on measures applicable to notification of personal data breaches;

- Methodical Instruction of the Regulatory Authority for the notification of the personal data breach; and
- Concept of cybersecurity in the Slovak Republic.

48.7 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/uoou/en

For more information, contact:

Name:	Peter Bartoš
Firm:	Ružička Csekes, in association with CMS Austria
Address:	Vysoká 2/B, 811 06 Bratislava, Slovakia
Telephone:	+421 2 3233 3444
Fax:	+421 2 32 33 34 43
Email:	peter.bartos@rc-cms.sk
Website:	www.rc-cms.sk

49. SLOVENIA[30]

49.1 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") of any personal data breach.

If, however, the data breach constitutes a criminal offence that 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 complaint with the prosecution authorities.

Nonetheless, if the data breach occurs in connection with a publicly available electronic communications service, the provider of the public electronic communications service 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.

49.2 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 personal data. Personal data is any data relating to an individual, irrespective of the form in which it is expressed. The breach relates to the personal data under the above definition.

As 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 and/or a natural person or legal entity who has notified the competent regulatory authority of the relevant services. The notification of the Communications Agency is obligatory irrespective of the severity of the breach. 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 to the affected individual is not required.

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

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

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

A failure to report 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.

If the provider of the electronic communication service did not inform the affected individual of the breach, the Communications Agency can, after examining the possible negative effects of such breach, instruct the provider to inform the individual of the breach.

A failure to notify of a breach through the publicly available electronic communication service may result in a fine from EUR 50,000 to EUR 400,000 for the service provider as a legal entity and a fine from EUR 500 to EUR 10,000 for the legal representative of the legal entity. A lower fine is prescribed for sole proprietors and legal entities regarded as micro or small undertakings in accordance with the Act governing companies.

49.5 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 notification of 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-2), 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.

49.6 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.

49.7 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, SI-1000 Ljubljana, Slovenia
Telephone:	+386 0 1 230 9730
Fax:	+386 0 1 230 9778
Email:	gp.ip@ip-rs.si
Website:	www.ip-rs.si

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

Name:	Agency for communication networks and services of the Republic of Slovenia (Agencija za komunikacijska omrežja in storitve Republike Slovenije
Address:	Stegne 7, SI-1000 Ljubljana, Slovenia
Telephone:	+386 1 5836 300
Fax:	+386 1 5111 101
Email:	info.box@akos-rs.si
Website:	www.akos-rs.si/akos-ang

For more information, contact:

Name:	Luka Fabiani
Firm:	CMS Slovenia
Address	Bleiweisova 30, SI-1000 Ljubljana, Slovenia
Telephone:	+386 1 6205 210
Fax:	+386 1 6205 211
Email:	luka.fabiani@cms-rrh.com
Website:	www.cms-rrh.com

50. SOUTH KOREA

50.1 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 Utilisation 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 case, be either 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 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.

50.2 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 PIPA, the notification duties arise when the data breach occurs. As mentioned in the answer to Question 50.1 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 PIPA as data that pertains to a living person, such as the name, resident registration number and 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.

50.3 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 PIPA and the IT Network Act, should include a description of the breached personal information, when and how the breach occurred, 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.

50.4 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.

50.5 Even if there is no current legal obligations 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)?

If the data breach affects residents in Korea, notice to the affected individuals and the regulator is "required," and this is the case even where both the data controller and the data processor are located outside of Korea. For example, under the IT Network Act, a foreign retailer operating a website directed to Korean residents with its server hosted by another company located outside of Korea will be subject to the notice requirements in the event of a data breach.

50.6 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 PIPA, the most prominent Korean data protection law is the IT Network Act, which governs the relationships between IT service providers and their users.

50.7 Contact information for Data Protection Authority:

Name: MOI (Ministry of the Interior)
Address: 209 Sejong-daero (Sejong-ro), Jongno-gu, Seoul, Korea
Telephone: +82 2 2100 3399
Website: www.moi.go.kr

Name: KISA (Korea Internet Security Agency)
Address: IT Venture Tower, Garak-dong 78, Songpa-gu, Korea 05717
Telephone: +82 2 405 5118
Website: www.kisa.or.kr

Name: NIA (National Information Security Agency)
Address: 53, Cheomdan-ro, Dong-gu, Daegu, Korea, 41068
Telephone: +82 53 2131 0114
Email: ict@nia.or.kr
Website: www.nia.or.kr

Name: KCC (Korea Communications Commission)
Address: 47, Gwanmun-ro, Gwacheon-si, Gyeonggi-do, 13809, Republic of Korea
Telephone: +82 2 500 9000
Email: webmaster@kcc.go.kr
Website: www.kcc.go.kr

For more information, contact:

Name: Taeuk Kang
Firm: Bae, Kim & Lee LLC
Address: 133 Teheran-ro, Gangnam-gu, Seoul, Republic of Korea 06133
Telephone: +82 2-3404 0475
Fax: +82 23404 0805
Email: taeuk.kang@bkl.co.kr
Website: www.bkl.co.kr

51. SPAIN[31]

51.1 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 or the DPA. Under the Regulation referred to in the answer to question 51.6 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.

Specific breach notification requirements apply to providers of public electronic communications services.[32]

51.2 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.

51.3 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 Breach Record" referred to in Question 51.1 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 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.

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

Not applicable.

---

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

[32] Under the Spanish Telecommunications Act (Law 9/2014, of 9 May), public electronic communications service providers must notify the DPA and their customers (with some exceptions in this last case) of any data breaches (article 41.3), and also the relevant Ministry when the data breach impacted significantly on the telecommunication network or on their service (article 44.3).

51.5 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 depends on the nature of the breach, the type and volume of the data involved, whether it is encrypted, whether the breach is 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 any data breaches. Then the DPA would be much more likely to cooperate with the company than if the data breach were discovered through a complaint or a report in the media.

In any case, whether the controller is established in Spain or not, we recommend that the issue is appropriately handled from the beginning, by informing the individuals affected, instead of waiting to be sued by the data subjects, particularly when the company must inform individuals of the same data breach in other jurisdictions.

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

The main national data protection laws and regulations are:

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

51.7 Contact information for Data Protection Authority

Name:	Spanish Data Protection Authority (Agencia Espanola de Proteccion de Datos)
Address:	C/ Jorge Juan 6, 28001 Madrid, Spain
Telephone:	+34 90 1100 099
Fax:	+34 91 2663 517
Email:	See website
Website:	www.agpd.es

For more information, contact:

Name:	Albert Agustinoy
Firm:	Cuatrecasas, Gonçalves Pereira
Address:	Paseo de Gracia 111, 08008 Barcelona, Spain
Telephone:	+34 93 2905 585
Fax:	+34 93 2905 569
Email:	albert.agustinoy@cuatrecasas.com
Website:	www.cuatrecasas.com

52. SWEDEN[33]

52.1 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 of 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.

52.2 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.

52.3 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.

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

Not applicable.

52.5 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)?

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 personal data.

Such measures could be to inform the data subjects to change their passwords 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.

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

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

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

52.7 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:	+46 08 652 86 52
Email:	datainspektionen@datainspektionen.se
Website:	www.datainspektionen.se

For more information, contact:

Name:	Bobi Mitrovic or Fredrik Roos
Firm:	Setterwalls Advokatbyrå AB
Address:	Sankt Eriksgatan 5, P.O. Box 11235, SE-404 25, Gothenburg, Sweden
Telephone:	+46 31 701 1700
Fax:	+46 31 701 1701
Email:	bobi.mitrovic@setterwalls.se or fredrik.roos@setterwalls.se
Website:	www.setterwalls.se

53. SWITZERLAND

53.1 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 an explicit obligation to notify individuals or the Federal Data Protection and Information Commissioner ("FDPIC"). However, an obligation to notify individuals may arise from:

- The principle that persons processing personal data have to observe the rules of good faith (Art. 4 para. 2 FDPA);
- The general obligation to mitigate damages; or
- 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.

53.2 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 53.1 above may, in principle, also apply to data processors.

53.3 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.

53.4 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).

53.5 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, and whether data security requires a notification.

53.6 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.

53.7 Contact information for Data Protection Authority:

Name:	Federal Data Protection and Information Commissioner
Address:	Feldeggweg 1, 3003 Bern, Switzerland
Telephone:	+41 31 322 4395
Fax:	+41 31 325 9996
Website:	www.edoeb.admin.ch

For more information, contact:

Name:	Dr. Robert G. Briner
Firm:	CMS Switzerland
Address:	Dreikönigstrasse 7, 8002 Zurich, Switzerland
Telephone:	+41 44 285 1111
Fax:	+41 44 285 1122
Email:	robert.briner@cms-veh.com
Website:	www.cms-veh.com

54. TAIWAN

54.1 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)?

Where the personal data is stolen, disclosed, altered or infringed in any other way due to the breach of the Personal Information Protection Act ("PIPA"), the data controller/processor is required by Article 12 of PIPA to notify the affected data subject. However, it is not required to notify the regulator.

54.2 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?

Whenever any personal data is breached, a proper notification must be given after investigation in accordance with Article 12 of PIPA. Personal data includes name, date of birth, ID 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 that may be used to identify a living natural person, either directly or indirectly, as defined in Article 2 of PIPA.

For the purpose of PIPA, a data processor shall be deemed a data controller as set forth in Article 4 PIPA. The provisions of PIPA shall apply to the data controller and the data processor to the same extent. As a result, both the data controller and the data processor are bound by the notification obligation.

54.3 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?

It is required by Article 22 of the Enforcement Rules of PIPA that the content of the notice shall include the fact of the infringement and the countermeasures that have been taken. Though there is no timeline for the notification in PIPA, it is required by Article 22 of the Enforcement Rules that such notification be given promptly (after conducting the necessary investigation and taking countermeasures).

It is further required by Article 12 PIPA that the notification shall be proper. According to Article 22 of the Enforcement Rules, a notification will be considered as proper if it is given promptly to the data subject verbally, in writing or via telephone, text message, email, facsimile, electronic document or in another manner that shall be sufficient to make or be likely to make the data subject informed of such notification. However, if such notification costs too much, after taking

into account technical feasibility and privacy protection of the data subject, such notification may be made via the internet, news media or other proper public means.

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

Where a data controller/processor fails to give a breach notification in accordance with Article 12 PIPA, the competent authority may, under Article 48 PIPA, order the breaching data controller/processor to take corrective measures within a specified period of time; failure to comply with such order shall be subject to an administrative fine ranging from NTD 20,000 to NTD 200,000 for each failure. In addition, the legal representative of such data controller/processor shall be subject to the same amount of administrative fine unless he proves that he has fulfilled his obligation to prevent such breach from occurring.

Further, in the event of any breach of PIPA, including failure to give notification that could have prevented or minimized damages, either pecuniary or non-pecuniary, to the data subject, a data controller/processor shall compensate for such damages unless the data controller/processor proves that it has no negligence in the breach (i.e., negligence is presumed). If such damages are hard to or cannot be proved, an amount of NTD 500 to NTD 20,000 may be awarded per data subject per event, subject to an aggregate amount of NTD 200 million or the amount of benefits derived from such breach, whichever is higher.

54.5 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)?

PIPA also applies to any data controller or data processor that collects, processes, uses or transmits, outside of Taiwan, the personal data of Taiwanese nationals (Article 51 PIPA). As a result, a legal obligation to give breach notification applies to these controllers/processors.

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

PIPA is the main body of law governing data protection in Taiwan. Its Enforcement Rules help clarify or implement its provisions.

54.7 Contact information for Data Protection Authority:

There is no single data protection authority. The various central Ministries and city/county governments serve as the competent authorities of data protection within their own jurisdictions. For example, the Financial Supervisory Commission is the competent authority of data protection for financial services industries, while the Ministry of Economic Affairs is for general corporations.

For more information, contact:

Name:	Chun-yih Cheng
Firm:	Formosa Transnational Attorneys at Law
Address:	13th Floor, Lotus Building, 136 Jen Ai Road Section 3, Taipei 10657, Taiwan
Telephone:	+886 2 2755 7366
Fax:	+886 2 2708 6035
Email:	chun-yih.cheng@taiwanlaw.com
Website:	www.taiwanlaw.com

55. THAILAND

55.1 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 specific obligations under Thai law to notify either affected individuals or regulators in the case of a data breach. Thailand does not have a single specific law that provides for personal data protection, although a draft Data Protection Bill has been in the legislative process since 2009. More stringent regulations in regard to data protection, storage and notice requirements are sector specific.

55.2 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.

55.3 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.

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

There are no statutory penalties or fines for not reporting a data breach. Several laws contain penalties for unauthorised use of certain information. The Credit Information Act B.E. 2545, as amended, imposes fines and penalties on the unauthorised disclosure of personal credit information and on any data controller that fails to implement proper security measures to protect personal data.

55.5 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)?

We recommend that individuals are notified of breaches, depending on the severity, and that data controllers take action to limit any adverse effects of such breach to limit civil liability. This is particularly important in the case of personal data that may cause reputational damage, as well as financial losses to that individual.

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

Section 4 of the current Interim Constitution B.E. 2557 (2014) provides that human dignity, rights, liberties and equality of the people shall be protected by the constitutional convention and by Thailand's international obligations. In addition, protections included under the Thai

Penal Code, Child Protection Act and regulations for certain sectors (telecommunication, banking and financial institutions) that require "appropriate" levels of data security, and protect against unauthorised collection or use of certain personal data. Other relevant regulations that provide data protection guidelines include the following:

(a) Civil and Commercial Code

The use or disclosure of personal data without consent from the personal data owner may be considered a wrongful act under the CCC if the use or disclosure is committed with either a specific intent to harm the data owner unlawfully, or through negligence. The wrongdoer shall be responsible for compensation arising out of the wrongful use or disclosure.

(b) Computer Crimes Act

This Act lays out general prohibitions on the use, storage and distribution of electronic information, as well as penalties for use of data that is collected through fraudulent means, use of personal data that would damage reputation, or generally use of data that is not permitted under the laws of Thailand. The Act allows for criminal prosecution for violations of the regulations and requirements listed therein.

(c) The Official Information Act

Provisions in the Official Information Act of Thailand seek to protect private persons against state interference with their private information and allow the state to collect certain information in the interest of national security.

(d) Labour Protection Act

Under Section 113 of the Labour Protection Act, an employer must collect the following information from its employees:

(i) Name and surname,

(ii) Sex,

(iii) Nationality,

(iv) Date of birth or age,

(v) Current address,

(vi) Date of commencement of employment,

(vii) Position or job duties,

(viii) Wage rate and other fringe benefits which the employer has agreed to give to the employee, and

(ix) Date of expiry of employment.

Under Section 115 of the Labour Protection Act, an employer must retain these records for not less than two years from the date the employee's employment terminated.

(e) Credit Information Business Act

This Act provides regulations for the collection, storage and use of individuals' credit information by companies that are permitted to conduct such business activities. The Act stipulates consent and data retention/storage requirements (note that the Act merely stipulates that such storage must be "appropriate", as well as limitations on the type of data that may be collected or disseminated by such credit data collectors.

(f) Draft Data Protection Bill

This Bill, in its current draft, includes more stringent measures and controls in regard to the collection, use, storage and dissemination of personal data than what currently exists. The Bill defines personal data as, "specific data of a natural person; e.g., educational report, financial report, health report, criminal report, working report, activities of well-known persons or any number, codes or any means that may be made to identify such persons, such as fingerprints, human sound recordings, photos, including specific data of deceased persons." Further, the Bill includes a definition of "Personal Data Collector," as the person who undertakes responsibility in compiling, controlling the use, and managing the disclosure of the personal data according to the law.

The Personal Data Controller shall not compile, use or disclose the personal data of other persons without prior consent having been provided by the owner of the data, except in cases outlined by this Bill or where other laws provide otherwise.

In seeking the consent from the owner of the personal data, the Personal Data Controller shall specify the purposes of the compilation, usage or disclosure of the data. Such consent shall not be acquired from the personal data owner through deceiving or misleading statements about the purpose of such action. The Data Protection Committee, which will be elected and appointed after the Bill comes into effect, may specify the form or content from which the Personal Data Controller seeks the form/content of the consent.

The personal data owner may, at any time, withdraw the consent he or she has given, unless such withdrawal is prohibited by law or through agreement, or the Personal Data Controller has caused the personal data to be unidentifiable or irrelevant to the owner of the personal data. However, should the withdrawal of consent have any consequences upon the personal data owner, the Personal Data Controller shall inform the personal data owner of the consequence of such withdrawal.

Note that the draft Bill has been under consideration for a number of years.

55.7 Contact information for Data Protection Authority:

Not applicable.

For more information, contact:

Name:	Niwes Phancharoenworakul or Christopher Kalis
Firm:	Chandler & Thong-ek Law Offices
Address:	7th-9th Fl., Bubhajit Building, 20 North Sathorn Rd, Bangkok 10500, Thailand
Telephone:	+662 266-6485 thru 6510
Fax:	+662 266-6483, 266-6484
Email:	niwes@ctlo.com or chris@ctlo.com
Website:	www.ctlo.com

56. TURKEY

56.1 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 Turkish law, no specific notification requirement applies in the event of data breaches. However, with respect to (a) above, an organization should make its own assessment about whether such a notification would be useful to minimize the effects of a potential claim in the future for damages incurred by affected individuals.

56.2 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.

56.3 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.

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

Not applicable.

56.5 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. Articles 135 and 136 of the Turkish Criminal Code stipulate that criminal offences of unlawful recording of personal data and obtaining personal data unlawfully are punishable by imprisonment for one to three years, and two to four years, respectively. In this respect, since a data breach may constitute one of the foregoing crimes, it is advisable to notify the public prosecutors of such incidents, as public prosecutors have the exclusive authority to investigate and prosecute individuals committing such offences.

As for credit card data information, Article 23 of the Law on Bank Cards and Credit Cards states that the entities or individuals providing services or selling goods to the customers cannot disclose, store or copy any customer information obtained through the customers' usage of their cards in the relevant workplaces, and infringements of this obligation are punishable by imprisonment from one to three years.

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

The primary piece of legislation for the protection of data is Paragraph 3 of Article 20 of the Constitution of the Republic of Turkey, which states: "Every individual has the right to request the protection of his or her personal data. This right encompasses being informed about the personal data held, being able to access the data, and being able to request that the data be corrected or deleted. Personal data shall only be processed under the circumstances designated by the law or through the full consent of the concerned person. Principles and procedures regarding the protection of personal data shall be prescribed by law." However, this legislation does not introduce a notification requirement in case of a breach.

Turkey ratified the Council of Europe's Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data ("Convention No. 108") on 18 February 2016. Convention No. 108 now has the force of law in Turkey. Some principles that made their way into Turkish domestic legislation through ratification of Convention No. 108 are as follows: (i) companies should not store any personal data other than what is required for the legitimate purpose or use of such data and (ii) companies should not store such data for longer than is necessary.

There has been a draft law pending before Parliament since 2008, titled the "Law for the Protection of Personal Data", which has been prepared to meet Turkey's obligations under Convention No. 108 and which is in line with the EU Directive 95/46/EC. The draft law, which is expected to be enacted soon, foresees the establishment of a committee (namely, the Personal Data Protection Committee), which will have the exclusive duty to process and accept all applications to be made with respect to breaches related to personal data issues. The draft law also imposes an obligation on data controllers to notify the Personal Data Protection Committee as well as the relevant individuals in the event that any processed personal data is obtained by third parties.

Notwithstanding the foregoing, data protection matters are also partially regulated throughout different pieces of legislation under Turkish law, including:

- Article 75 of the Labour Code states that employers are obliged to follow good faith principles in disclosing personal information of their employees;
- Article 419 of the Turkish Code of Obligations sets forth that an employer is allowed to utilise employees' personal data only to the extent it is required for performance of the employment agreement or the disposition of the employee towards his/her work; and
- Article 73 of the Banking Law determines that customers' personal data must be kept confidential by the banks personnel and any other persons who have become aware of such personal data due to the nature of their occupations. Infringement of such obligation is punishable by administrative fine and imprisonment for one to three years, depending on the particulars of the offence.

56.7 Contact information for Data Protection Authority:

Not applicable.

For more information, contact:

Name: Kemal Mamak or Kayra Üçer
Firm: Hergüner Bilgen Özeke Attorney Partnership
Address: Büyükdere Caddesi 199, Levent 34394, Istanbul, Turkey
Telephone: +90 212 310 1800
Fax: +90 212 310 1899
Email: kmamak@herguner.av.tr or kucer@herguner.av.tr
Website: www.herguner.av.tr

57. UKRAINE

57.1 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 Ukrainian Parliament Commissioner for Human Rights who performs the functions of a data protection authority ("DPA"). The law only provides for the right of the individual owner of the personal data to inform the DPA about the facts of the personal data breach affecting him/her and apply for protection of his/her rights. At the same time, the DPA has the right to carry out investigations and inspections. 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.

57.2 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 any personal data may serve as the reason for a notification submission to the DPA. 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 and 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 a 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.

57.3 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 for damages caused by the breach are possible only within the respective statutes of limitations. The infringer may be subject to

administrative sanctions no later than two months after the breach or after the exposure of the breach (in case of a continuing violation). The respective term of limitation for criminal liability is three or five years (depending on the qualification of the violation). Compensation for damages through civil proceedings may be possible with application of the standard three-year statute of limitation. The notification should be sent by regular mail or filed directly with the relevant authority in written form.

57.4 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.

57.5 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.

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

- Law of Ukraine "On Personal Data Protection" no. 2297-VI, dated 1 June 2009, as amended;
- Criminal Code of Ukraine no. 2341-III dated 5 April 2001, as amended; and
- Code of Administrative Offences no. 8073-X dated 7 December 1984, as amended.

57.7 Contact information for Data Protection Authority:

Name:	Ukrainian Parliament Commissioner for Human Rights
Address:	21/8 Instytutska St., 01008 Kyiv City, Ukraine
Telephone:	+380 44 2531 135; +380 44 2535 394; +380 44 2538 194
Email:	hotline@ombudsman.gov.ua
Website:	www.ombudsman.gov.ua

For more information, contact:

Name:	Maria Orlyk or Kateryna Soroka
Firm:	CMS Ukraine
Address:	19-B Instytutska, 5th Floor, 01021 Kyiv, Ukraine
Telephone:	+380 44 5001 710 or +380 44 5001 711
Fax:	+380 44 5001 716
Email:	maria.orlyk@cms-rrh.com or kateryna.soroka@cms-rrh.com
Website:	www.cms-rrh.com

58. UNITED KINGDOM[34]

58.1 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 either affected individuals or the DPA of data breaches.

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").

58.2 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 58.1 above.

58.3 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

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

of the breach, the provider's contact details and suggestions on how to mitigate the breach. The Information Commissioner recommends that the service provider submit 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.

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

As there is no requirement to notify (other than electronic communications service providers under PECR), there is no specific penalty or fine for failing to notify. However, for breaches of the Data Protection Act (including for example, personal data breach of security requirements), the Information Commissioner can issue monetary penalties against data controllers of up to GBP 500,000 for serious breaches of the Data Protection Act and enforcement notices. The Information Commission may also require undertakings (although this is not an official remedy under the Data Protection Act). 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 GBP 1,000 under PECR.

58.5 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.

58.6 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.

58.7 Contact information for Data Protection Authority:

Name:	Information Commissioner's Office
Address:	Wycliffe House, Water Lane, Wilmslow, Cheshire, United Kingdom SK9 5AF
Telephone:	+44 30 3123 1113 or +44 16 2554 5745
Fax:	+44 16 252 4510
Email:	casework@ico.org.uk
Website:	www.ico.org.uk

For more information, contact:

Name:	Kirsten Whitfield
Firm:	Gowling WLG
Address:	Two Snowhill, Birmingham, B4 6WR, United Kingdom
Telephone:	+44 (0)37 0903 1000
Fax:	+44 (0) 37 0904 1099
Email:	kirsten.whitfield@gowlingwlg.com
Website:	www.gowlingwlg.com

59. UNITED STATES

59.1 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 require notice to be provided to affected individuals in the event of a data breach. Fifty-one U.S. jurisdictions, including 47 states, the District of Columbia, Guam, Puerto Rico and the U.S. Virgin Islands, have enacted data breach notification laws. (As of the date of this publication Alabama, New Mexico, and South Dakota lack data breach notification statutes, though the legislatures of both Alabama and New Mexico debated, but did not pass, data breach legislation in 2015).

In addition to such state data breach notification requirements, companies in certain regulated industries, such as banking and health care, are also subject to certain state and federal industry-specific breach notification requirements. Compliance with federal industry-specific requirements often 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 databases.

The United States does not have a single data protection authority. That said, 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.

59.2 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 state data breach notification requirements are similar, they contain significant variations. Determining what state law applies typically depends 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.

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, health care 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 licence or government-issued identification number;
- Financial account information;

or, depending on the law or regulation triggered:

- Other government identification information that could be used for identity theft;
- User names and passwords, access codes or security questions and answers that would allow access to an online account (whether or not the individual's name is also compromised);
- Unique biometric data; or
- Medical information or health insurance information.

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.

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.

Most U.S. breach notification requirements are not defined in terms of "data controllers" or "data processors," as those terms are not used in the U.S. legal system. It is the entity that owns, licences, 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, licences, 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.

59.3 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. For instance, Florida requires notification to be made within 30 days of discovering the breach. Other states, such as Ohio, Vermont and Wisconsin, require that notice be provided to affected individuals within 45 days of discovering the breach. California's health care breach notification rules require relevant agencies and individuals to be provided notice no later than fifteen business days after discovery of a breach.

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

Governmental agencies, including state Attorneys General and the U.S. Department of Health and Human Services, 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 when 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"). Exposure also increases when companies fail to adhere to their own published data security policies. The Federal Trade Commission (FTC) has brought enforcement actions against companies following breaches pursuant to Section 5 of the Federal Trade Commission Act that allows it to take action against unfair or deceptive practices. The FTC's authority to take civil action against companies that fail to maintain adequate data security systems was recently upheld in the landmark Third Circuit Court of Appeals case, *FTC v. Wyndham Worldwide Corp.* (2015). In that case, and in other enforcement actions, the FTC interprets "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.

59.5 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 59.2 above, U.S. legal terminology does not refer to a "data controller" or a "data processor," but because there are many state and federal breach notification requirements, almost any breach of Personal Information will likely require some sort of notification, in the absence of an exception. Even for breaches affecting residents of the three states that do not currently require notification to affected individuals (Alabama, 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 potentially material information to be disclosed under existing securities law disclosure requirements and accounting standards applicable to publicly traded companies.

Though a wide-reaching national breach notification statute does not yet exist, it is an issue that is regularly debated in Congress, particularly in the wake of an increasing list of high-profile data breaches. Though opposed by many state governments and advocacy groups who fear that a national standard will undermine the ability of individual states to impose strong data security regulations on companies that serve their residents, it is possible that a uniform national data breach statute could be passed in the near future.

59.6 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/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx.

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

- Banking: Interagency Guidance on Response Programs for Unauthorised 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 licences (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, 18 August 2010; Ohio Insurance Bulletin 2009-12; Rhode Island Insurance Division Regulation 107; Wisconsin Insurance Bulletin dated 4 December 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, in some cases, the media by vendors of personal health records ("PHR") and PHR-related entities in the event of a data breach involving 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 Locke Lord 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 Locke Lord Privacy and Cybersecurity Practice Group's website to view the most recent edition.

59.7 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 59.6 above.

For more information, contact:

Name: Mark E. Schreiber
Firm: Locke Lord LLP
Address: 111 Huntington Avenue, Boston, Massachusetts USA 02199
Telephone: +1 617 239 0585
Email: mark.schreiber@lockelord.com
Website: www.lockelord.com

Name: Theodore P. Augustinos or Karen L. Booth
Firm: Locke Lord LLP
Address: 20 Church Street, Hartford, Connecticut USA 06103
Telephone: +1 860 541 7710 or +1 860 541 7714
Email: ted.augustinos@lockelord.com or karen.booth@lockelord.com
Website: www.lockelord.com

Name: Julie M. Engbloom and Darin M. Sands
Firm: Lane Powell PC
Address: 601 SW Second Avenue, Suite 2100, Portland, Oregon USA 97204-3158
Telephone: +1 503 778 2183 or +1 503 778 2117
Email: engbloomj@lanepowell.com or sandsd@lanepowell.com
Website: www.lanepowell.com

60. URUGUAY

60.1 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)?

According to Uruguayan Data Protection Law, the processor or the person responsible for a database or of its use must inform the affected parties of the occurrence of any security breach incident that may affect significantly their rights. No notification to government authorities is required, unless it is required by sector-specific regulation (such as in the case of financial institutions where specific regulations provide that any event or circumstance not frequent or regular, which may materially affect the business or the institution's economic or legal situation, shall be notified to the Central Bank of Uruguay at the latest within two days following the day of its occurrence or from the day that the event came to the institution's knowledge).

60.2 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?

Applicable regulations do not provide for a specific procedure to be followed. Therefore, in case of a security breach incident related to personal data that significantly affects the rights of the parties involved, it will be enough to notify the affected parties of such breach.

60.3 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.

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

There are not specific sanctions related to failing to notify a security breach incident; however, general sanctions would apply. The sanctions that the Personal Data Regulatory and Control Unit ("Unidad Reguladora y de Control de Datos Personales" or "DPA") may apply are the following:

- A warning;
- A fine of up to five hundred thousand indexed units (approx. USD 55,000);
- A five-day suspension of the relevant database;
- The cancellation of the database.

60.5 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)?

Please refer to our answer to Question 60.1.

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

Law N° 18.331 and its regulatory Decree N° 414/009 established in Uruguay a general regulatory framework with the purpose of assuring the fundamental right of protection of personal data and intimacy/privacy. The Uruguayan regulatory framework applies if: (a) the responsible party for the database or of its processing is located in Uruguay; or (b) the responsible party for the database or of its processing is located outside Uruguay but uses for such processing means located in Uruguay (e.g., servers hosted in Uruguay).

In order to assure compliance with said regulatory framework, the Uruguayan Data Protection Authority issued certain Resolutions, which are binding to data controllers. Some of these regulations are:

- Resolution 17/009, dated 15 June 2009, which sets forth that under certain circumstances personal data may be transferred to EU countries as well as to non-EU countries that, according to the European Commission, ensure an adequate level of protection for personal data without the need to obtain prior authorization from the DPA; and

- Resolution 105/015, dated 23 December 2015, which specifies the applicable sanctions by reference to the seriousness of the breach.

60.7 Contact information for Data Protection Authority:

Name:	Unidad Reguladora y de Control de Datos Personales
Address:	Andes N° 1365, 7th floor, Montevideo, 11000, Uruguay
Telephone:	+598 2901 0065 option 3
Email:	infocdp@agesic.gub.uy
Website:	www.datospersonales.gub.uy

For more information, contact:

Name:	Florencia Castagnola or Sofía Anza
Firm:	Guyer & Regules
Address:	Plaza Independencia 811, 11000 Montevideo, Uruguay
Telephone:	+598 2902 1515
Fax:	+598 2902 5454
Email:	fcastagnola@guyer.com.uy or sanza@guyer.com.uy
Website:	www.guyer.com.uy

LIST OF CONTRIBUTORS

Argentina

Name: Carlos E. Alfaro
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
Website: www.alfarolaw.com

Australia

Name: Veronica Scott
Firm: MinterEllison
Address: Rialto Towers, 525 Collins Street, Melbourne, VIC 3000, Australia
Telephone: +61 3 8608 2126 or +61 3 8608 2654
Fax: +61 3 8608 1181 or + 61 3 8608 1000
Email: veronica.scott@minterellison.com
Website: www.minterellison.com

Austria

Name: Robert Keisler or Dr. Bernt Elsner
Firm: CMS Austria
Address: Gauermanngasse 2, 1010 Vienna, 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

Name: Tom Heremans and Tom De Cordier
Firm: CMS Belgium
Address: Chaussee de La Hulpe 178, B-1170 Brussels, Belgium
Telephone: +32 2 743 6973
Fax: +32 2 743 6901
Email: tom.heremans@cms-db.com / tom.decordier@cms-db.com
Website: www.cms-db.com

Bosnia and Herzegovina

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

Brazil

Name: Marcela Waksman Ejnisman or Felipe Borges Lacerda Loiola
Firm: TozziniFreireAdvogados
Address: Rua Borges Lagoa, 1328, Sao Paulo, SP, 04038-904, Brazil
Telephone: +55 11 5086 5000
Fax: + 55 11 5086 5555
Email: mejnisman@tozzinifreire.com.br or fblacerda@tozzinifreire.com.br
Website: www.tozzinifreire.com.br

Bulgaria

Name: Marin Drinov
Firm: CMS Bulgaria
Address: 4 Knyaz Alexander I Battenberg Str., fl. 2, 1000 Sofia, Bulgaria
Telephone: +359 2 447 1317
Fax: +359 2 447 1390
Email: marin.drinov@cms-rrh.com
Website: www.cms-rrh.com

Canada

Name: Peter Ruby or Rachel Ouellette
Firm: Goodmans LLP
Address: Bay Adelaide Centre, 333 Bay Street, Suite 3400 Toronto, Ontario, Canada, M5H 2S7
Telephone: +1 416 979 2211
Fax: +1 416 979 1234
Email: pruby@goodmans.ca or rouellette@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

Name: Sergio Orrego Flory
Firm: Urenda Rencoret Orrego y Dörr
Address: Avenida Andres Bello No 2711, Piso 16, Las Condes, Santiago de Chile, Santiago, Chile, 7550611
Telephone: +56 2 2499 5500 or +56 2 499 5507
Fax: +56 2 2499 5555
Email: sorrego@urod.cl
Website: www.urod.cl

China

Name: Michael Shu
Firm: Zhong Lun Law Firm
Address: 10-11/F, Two IFC, 8 Century Avenue, Pudong New Area, Shanghai 200120, People's Republic of China
Telephone: +86 21 6061 3650
Fax: +86 21 6061 3555
Email: michaelshu@zhonglun.com
Website: www.zhonglun.com

Colombia

Name: Diego Cardona
Firm: Philippi, Prietocarrizosa, Ferrero DU & Uría
Address: Carrera 9 # 74-08, Bogota D.C., Colombia
Telephone: +571 326 8600 Ext. 1419
Fax: +571 326 8419
Email: diego.cardona@ppulegal.com
Website: www.ppulegal.com

Costa Rica

Name: Valeria Aguero
Firm: Arias & Muñoz
Address: Costa Rica, Centro Empresarial Forum 1, Edificio C, oficina 1C1.
Telephone: +506 2503 9873
Fax: +506 2204 7580
Email: vaguero@ariaslaw.co.cr
Website: www.ariaslaw.com

Croatia

Name: Marija Mušec
Firm: OdvjetniÐko društvo Bardek, Lisac, Mušec, Skoko d.o.o. in cooperation with CMS Austria
Address: Ilica 1, 10000 Zagreb, Croatia
Telephone: +385 1 4825-600
Fax: +385 1 4825-601
Email: marija.musec@bmslegal.hr
Website: www.bmslegal.hr

Czech Republic

Name: Karin Pomaizlova
Firm: TaylorWessing e|n|w|c advokati v.o.s.
Address: U Prasne brany 1, 110 00 Prague 1, Czech Republic
Telephone: +420 224 81 92 16
Fax: +420 224 81 92 17
Email: k.pomaizlova@taylorwessing.com
Website: www.taylorwessing.com

Denmark

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

El Salvador

Name: Morena Zavaleta
Firm: Arias & Muñoz
Address: Calle La Mascota #533, Colonia San Benito. San Salvador, El Salvador
Telephone: +503 2257-0900
Fax: +503 2257-0901
Email: morena.zavaleta@ariaslaw.com
Website: www.ariaslaw.com

European Union

Name: Christian Runte
Firm: CMS Germany
Address: Nymphenburger Straße 12, 80335 Munich, Germany
Telephone: +49 89 238 07 163
Fax: +49 89 238 07 40804
Email: christian.runte@cms-hs.com
Website: www.cms-hs.com

Finland

Name: Eija Warma or Anette Luomala
Firm: Castrén & Snellman Attorneys Ltd
Address: PO Box 233 (Eteläesplanadi 14), FI-00131 Helsinki, Finland
Telephone: +358 20 7765 376
Fax: +358 20 7761 376
Email: eija.warma@castren.fi or anette.luomala@castren.fi
Website: www.castren.fi

France

Name: Laure Marolleau
Firm: Soulier Avocats
Address: 50 Avenue de Wagram, 75017 Paris, France
Telephone: +33 1 4054 2929
Fax: +33 1 4054 2920
Email: l.marolleau@soulier-avocats.com
Website: www.soulier-avocats.com

Germany

Name: Christian Runte
Firm: CMS Germany
Address: Nymphenburger Straße 12, 80335 Munich, 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

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

Guatemala

Name: Pamela Jiménez
Firm: Arias & Muñoz
Address: Diagonal 6, 10-01 zona 10 Centro Gerencial Las Margaritas, Torre II, oficina 402-B. Ciudad de Guatemala, Guatemala, C. A.
Telephone: +502 2382 7700
Fax: +502 2382 7743
Email: pamela.jimenez@ariaslaw.com
Website: www.ariaslaw.com

Honduras

Name: Mario Agüero
Firm: Arias & Muñoz
Address: San Pedro Sula, Edificio Park Plaza, Local 19, Barrio Guamilito, 5° y 6° Calle, 11 Avenida N.O. San Pedro Sula, Cortes, Honduras
Telephone: +504 2550-2202
Fax: +504 2557-6488
Email: mario.aguero@ariaslaw.com
Website: www.ariaslaw.com

India

Name: Bomi Daruwala
Firm: Vaish Associates Advocates
Address: 106, Peninsula Centre, Dr. S. S. Rao Road, Parel, Mumbai, India – 400012
Telephone: +91 22 4213 4101
Fax: +91 22 4213 4102
Email: bomi@vaishlaw.com
Website: www.vaishlaw.com

Indonesia

Name: Richard Cornwallis
Firm: Makarim & Taira S.
Address: Summitmas I, 16th & 17th floors, Jl. Jend. Sudirman Kav. 61-62, Jakarta, Indonesia 12190
Telephone: + 6221 252 1272, 520 0001
Fax: +6221 252 2750, 252 2751
Email: richard.cornwallis@makarim.com
Website: www.makarim.com

Ireland

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

Name: Nurit Dagan
Law firm: 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

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

Name: Hitoshi Sakai
Firm: City-Yuwa Partners
Address: Marunouchi Mitsui Building, 2-2-2 Marunouchi, Chiyoda-ku, Tokyo, Japan 100-0005
Telephone: + 81 3 6212 5642
Fax: + 81 3 6212 5700
Email: hitoshi.sakai@city-yuwa.com
Website: www.city-yuwa.com

Luxembourg

Name: Héloïse Bock
Firm: Arendt & Medernach S.A.
Address: 41A, avenue J.F. Kennedy, L-2082 Luxembourg
Telephone: +352 40 7878 321
Fax: +352 40 7804 609
Email: heloise.bock@arendt.com
Website: www.arendt.com

Malaysia

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

Name: César G. Cruz Ayala or Diego R. Acosta Chin
Firm: Santamarina y Steta S.C.
Address: Ricardo Margain Zozaya 335, Piso 7, Col. Valle del Campestre, 66265 San Pedro Garza García, N.L., (Monterrey) México
Telephone: +52 81 8133 6002 or +52 81 8133 6018
Fax: +52 81 8368 0111
Email: ccruz@s-s.mx or dacosta@s-s.mx
Website: www.s-s.mx/site/eng

Mongolia

Name: Elisabeth Ellis
Firm: MinterEllison
Address: Suite 612 Central Tower, Great Chinggis Khaan's Square 2, Sukhbaatar District – 8, Ulaanbaatar, Mongolia
Telephone: +976 7700 7780
Fax: +976 7700 7781
Email: elisabeth.ellis@minterellison.com
Website: www.minterellison.com

Montenegro

Name: Milica PopoviĐ
Firm: CMS Montenegro
Address: Bulevar Džordža Vašingtona 3/22, 81000 Podgorica, Montenegro
Telephone: +382 20 416 070 / +381 11 320 8900
Fax: +382 20 416 071
Email: milica.popovic@cms-rrh.com
Website: www.cms-rrh.com

Mozambique

Name: Tomás Timbane
Firm: TTA Sociedade de Advogados
Address: Edifício Millennium Park, Torre A, Avenida Vladimir Lenine, nº 179, 6º Dtº, Maputo – Moçambique
Telephone: +258 843 141 820
Email: tomas.timbane@tta-advogados.com
Website: www.tta-advogados.com

Name: Miguel Spinola
Firm: PLMJ Sociedade de Advogados, RL
Address: Edifício Eurolex, Avenida da Liberdade, 224, 1250-148 Lisbon – Portugal
Telephone: +351 213 197 446 or +351 916 346 219
Fax: +351 21 319 74 00
Email: miguel.spinola@plmj.pt
Website: www.plmj.com

The Netherlands

Name: Hendrik Struik
Firm: CMS Netherlands
Address: Newtonlaan 203, 3584 BH Utrecht, The Netherlands
Telephone: +31 30 212 1726
Fax: +31 30 212 1157
Email: hendrik.struik@cms-dsb.com
Website: www.cms-dsb.com

New Zealand

Name: Richard Wells
Firm: Minter Ellison Rudd Watts Lawyers
Address: Lumley Centre, 88 Shortland Street, Auckland 1010, New Zealand
Telephone: +64 9 353 9908
Fax: +64 9 353 9701
Email: richard.wells@minterellison.co.nz
Website: www.minterellison.co.nz

Nicaragua

Name: Angélica Argüello
Firm: Arias & Muñoz
Address: Pista Jean Paul Genie, Edificio Escala, 3er piso, Managua, Nicaragua
Telephone: +505 2298 1360
Email: angelica.arguello@ariaslaw.com
Website: www.ariaslaw.com

Norway

Name: Halvor Manshaus
Firm: Advokatfirmaet Schjødt AS
Address: Ruseløkkveien 14, P.O.Box 2444 Solli, NO-0201 Oslo, Norway
Telephone: +47 23 01 1529
Fax: +47 22 83 1712
Email: hama@schjodt.no
Website: www.schjodt.no

Panama

Name: Siaska S.S.S. Lorenzo
Firm: Arias & Muñoz
Address: Torre Global, Piso 24, Oficina 2401, Calle 50, Panama City, Panama
Telephone: +507 282 1400
Fax: +507 282 1435
Email: siaska.lorenzo@ariaslaw.com
Website: www.ariaslaw.com

Peru

Name: Carlos A. Patron or Giancarlo Baella
Firm: Payet Rey Cauvi Perez Abogados
Address: Av. Victor Andres Belaunde 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 gbp@prc.com.pe
Website: www.prc.com.pe

Philippines

Name: Rolando V. Medalla, Jr. or Hiyasmin H. Lapitan
Firm: SyCip Salazar Hernandez & Gatmaitan
Address: SyCipLaw Center, 105 Paseo de Roxas, Makati City 1226, The Philippines
Telephone: +63 2 9823 500 or +63 2 9823 600, or +63 2 9823 700
Fax: +63 2 8173 145 or +63 2 8173 896
Email: rvmedalla@syciplaw.com or hhlapitan@syciplaw.com
Website: www.syciplaw.com

Poland

Name: Agata Szeliga or Katarzyna Paziewska
Firm: SołtysiĐski Kawecki & SzlĐzak
Address: ul. Jasna 26, 00-054 Warszawa, Poland
Telephone: +48 22 608 7006 or +48 22 608 7190
Fax: +48 22 608 7070
Email: agata.szeliga@skslegal.pl or katarzyna.paziewska@skslegal.pl
Website: www.skslegal.pl

Portugal

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

Name: Maxim Boulba
Firm: CMS Russia
Address: Gogolevsky Blvd. 11, 119019 Moscow, Russia
Telephone: +7 49 5786 4000
Fax: +7 49 5786 4001
Email: maxim.boulba@cmslegal.ru
Website: www.cmslegal.ru

Serbia

Name: Ksenija IvetiĐ or Radivoje PetrikiĐ
Firm: PetrikiĐ & Partneri AOD in cooperation with CMS Austria
Address: Cincar Jankova 3, 11000 Belgrade, 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

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

Slovakia

Name: Peter Bartoš
Firm: RužiĐka Csekes, in association with CMS Austria
Address: Vysoká 2/B, 811 06 Bratislava, Slovakia
Telephone: +421 2 3233 3444
Fax: +421 2 32 33 34 43
Email: peter.bartos@rc-cms.sk
Website: www.rc-cms.sk

Slovenia

Name: Luka Fabiani
Firm: CMS Slovenia
Address Bleiweisova 30, SI-1000 Ljubljana, Slovenia
Telephone: +386 1 6205 210
Fax: +386 1 6205 211
Email: luka.fabiani@cms-rrh.com
Website: www.cms-rrh.com

South Korea

Name: Taeuk Kang
Firm: Bae, Kim & Lee LLC
Address: 133 Teheran-ro, Gangnam-gu, Seoul, Republic of Korea 06133
Telephone: +82 2-3404 0475
Fax: +82 23404 0805
Email: taeuk.kang@bkl.co.kr
Website: www.bkl.co.kr

Spain

Name: Albert Agustinoy
Firm: Cuatrecasas, Gonçalves Pereira
Address: Paseo de Gracia 111, 08008 Barcelona, Spain
Telephone: +34 93 2905 585
Fax: +34 93 2905 569
Email: albert.agustinoy@cuatrecasas.com
Website: www.cuatrecasas.com

Sweden

Name: Bobi Mitrovic or Fredrik Roos
Firm: Setterwalls Advokatbyrå AB
Address: Sankt Eriksgatan 5, P.O. Box 11235, SE-404 25, Gothenburg, Sweden
Telephone: +46 31 701 1700
Fax: +46 31 701 1701
Email: bobi.mitrovic@setterwalls.se or fredrik.roos@setterwalls.se
Website: www.setterwalls.se

Switzerland

Name: Dr. Robert G. Briner
Firm: CMS Switzerland
Address: Dreikönigstrasse 7, 8002 Zurich, Switzerland
Telephone: +41 44 285 1111
Fax: +41 44 285 1122
Email: robert.briner@cms-veh.com
Website: www.cms-veh.com

Taiwan

Name: Chun-yih Cheng
Firm: Formosa Transnational Attorneys at Law
Address: 13th Floor, Lotus Building, 136 Jen Ai Road Section 3, Taipei 10657, Taiwan
Telephone: +886 2 2755 7366
Fax: +886 2 2708 6035
Email: chun-yih.cheng@taiwanlaw.com
Website: www.taiwanlaw.com

Thailand

Name: Niwes Phancharoenworakul or Christopher Kalis
Firm: Chandler & Thong-ek Law Offices
Address: 7th-9th Fl., Bubhajit Building, 20 North Sathorn Rd, Bangkok 10500, Thailand
Telephone: +662 266-6485 thru 6510
Fax: +662 266-6483, 266-6484
Email: niwes@ctlo.com or chris@ctlo.com
Website: www.ctlo.com

Turkey

Name: Kemal Mamak or Kayra Üçer
Firm: Hergüner Bilgen Özeke Attorney Partnership
Address: Büyükdere Caddesi 199, Levent 34394, Istanbul, Turkey
Telephone: +90 212 310 1800
Fax: +90 212 310 1899
Email: kmamak@herguner.av.tr or kucer@herguner.av.tr
Website: www.herguner.av.tr

Ukraine

Name: Maria Orlyk or Kateryna Soroka
Firm: CMS Ukraine
Address: 19-B Instytutska, 5th Floor, 01021 Kyiv, Ukraine
Telephone: +380 44 5001 710 or +380 44 5001 711
Fax: +380 44 5001 716
Email: maria.orlyk@cms-rrh.com or kateryna.soroka@cms-rrh.com
Website: www.cms-rrh.com

United Kingdom

Name: Kirsten Whitfield
Firm: Gowling WLG
Address: Two Snowhill, Birmingham, B4 6WR, United Kingdom
Telephone: +44 (0)37 0903 1000
Fax: +44 (0) 37 0904 1099
Email: kirsten.whitfield@gowlingwlg.com
Website: www.gowlingwlg.com

United States

Name: Mark E. Schreiber
Firm: Locke Lord LLP
Address: 111 Huntington Avenue, Boston, Massachusetts 02199 USA
Telephone: +1 617 239 0585
Email: mark.schreiber@lockelord.com
Website: www.lockelord.com

Name: Theodore P. Augustinos or Karen L. Booth
Firm: Locke Lord LLP
Address: 20 Church Street, Hartford, Connecticut 06103 USA
Telephone: +1 860 541 7710 or +1 860 541 7714
Email: ted.augustinos@lockelord.com or karen.booth@lockelord.com
Website: www.lockelord.com

Name: Julie M. Engbloom and Darin M. Sands
Firm: Lane Powell PC
Address: 601 SW Second Avenue, Suite 2100, Portland, Oregon 97204-3158 USA
Telephone: +1 503 778 2183 or +1 503 778 2117
Email: engbloomj@lanepowell.com or sandsd@lanepowell.com
Website: www.lanepowell.com

Uruguay

Name: Florencia Castagnola or Sofía Anza
Firm: Guyer & Regules
Address: Plaza Independencia 811, 11000 Montevideo, Uruguay
Telephone: +598 2902 1515
Fax: +598 2902 5454
Email: fcastagnola@guyer.com.uy or sanza@guyer.com.uy
Website: www.guyer.com.uy