2016 Global Data Breach Notification Guide
Global Data Breach Notification Guide
Editors’ Note

Global data breach notification requirements pose critical issues for legal departments, senior managers, and boards of companies in all industry sectors worldwide. The current environment creates a perfect storm with more data security threats, more vulnerabilities, and more data breach notification requirements.

The threats are diverse and ever-changing. Threat actors range from nation states pursuing economic gain or political aims, to individual hackers or collectives motivated by profit, challenge, or enjoyment, to employees or other insiders seeking revenge, financial reward, or other goals. The means of attack are also expanding, and range from spear phishing and social engineering, to man-in-the-middle and distributed denial of service (DDOS) attacks, and more. Intruders are searching for new and innovative ways to introduce malware into company systems, to steal, corrupt, or delete personal information, trade secrets, or other confidential information, and to otherwise cause harm.

The vulnerabilities are expanding as global organizations increasingly leverage data as a source of revenue and, in the process, expand the surface area for potential attacks. For example, the Internet of Things (IoT) enables companies to attach sensors associated with IP addresses to everything from home appliances to cars to pills that patients ingest. Companies are pursuing this connectivity as a business imperative to find new ways to track behavior, optimize resource consumption, utilize sensor-driven analytics, and monetize available data. Estimates indicate there will be as many as 50 billion devices connected to the Internet by 2020. That’s multiples of today’s numbers, such that there will be literally billions more sources of vulnerabilities.

Data breach notification requirements create significant corporate risk in this environment. Amidst the expansion of global threats and vulnerabilities, an increasing array of these data breach notification requirements are emerging around the world. California established the first data breach notification obligation in 2003 for a relatively narrow set of highly sensitive personal information including unencrypted Social Security Numbers and other government identifiers, financial account numbers (such as credit cards) and the corresponding security codes, and the like. Since then, California has expanded the range of data types covered by its law, and the vast majority of US states have enacted similar data breach notification laws. Non-US jurisdictions have also increasingly incorporated the concept of data breach notification into their “omnibus” data protection regimes that apply by their definitions to a broad range of information about identified or identifiable individuals. Many of these regimes establish short timelines to respond, duties
to notify regulatory authorities, and content and procedural rules for notification. Some of the emerging rules also apply to more than just unauthorized access, and can apply to unauthorized loss or processing, which may cover intrusions that destroy data and other activities that exceed authorized boundaries. In May 2018, the European Union’s General Data Protection Regulation (“GDPR”) will come into force and introduce sweeping data breach notification requirements that apply across all industry sectors.

The risks to companies in the context of a data breach are significant. Key concerns include reputational harm, adverse media attention, and customer churn, class actions and other claims from consumers, employees, corporate customers, financial institutions, and shareholders, and regulatory/law enforcement actions. As such, preparation is critical. Companies should address the potential for data security incidents throughout the full life cycle of information management, from product and application design, to initial data collection and use, to record retention and secure disposal. Companies should also proactively align incident response policies, legal counsel, forensic providers, identity theft protection services, public relations firms, and other resources to prepare for data incidents and notification issues.

Baker & McKenzie provides this **Global Data Breach Notification Guide** as a resource for companies to benchmark the ever expanding range of global breach notification requirements. As always, a guide is not a substitute for legal advice, and in the event of an actual or potential incident, companies need to engage qualified counsel to advise on the application of local breach notification and other requirements to their particular circumstances.


### Brian Hengesbaugh
Chair, Global IT/C Data Security Working Group
Baker & McKenzie’s Global IT/C Data Security Leadership Team

Lothar Determann (Palo Alto)
+1 650 856 5533
lothar.determann@bakermckenzie.com

Patrick Fair (Sydney)
+61 2 8922 5534
patrick.fair@bakermckenzie.com

Paul Forbes (Sydney)
+61 2 8922 5346
paul.forbes@bakermckenzie.com

Francesca Gaudino (Milan)
+39 02 76231 452
francesca.gaudino@bakermckenzie.com
Brian Hengesbaugh (Chicago)
+1 312 861 3077
brian.hengesbaugh@bakermckenzie.com

Theo Ling (Toronto)
+1 416 865 6954
theo.ling@bakermckenzie.com

Flavia Rebello (Sao Paulo)
+55 11 3048 6851
flavia.rebello@trenchrossi.com

Michael Stoker (Chicago)
+1 312 861 2870
michael.stoker@bakermckenzie.com
Global Data Breach Notification Guide

Associate Editor
Joan Melcar T. Tan (Manila)
+632 558 9421
joanmelcar.tan@bakermckenzie.com
Contributing Lawyers

Argentina
Guillermo Cervio
Buenos Aires
Tel: +54 11 4310 2223
guillermo.cervio@bakermckenzie.com

Roberto Grané
Buenos Aires
Tel: +54 11 4310 2214
roberto.grane@bakermckenzie.com

Australia
Anne-Marie Allgrove
Sydney
Tel: +61 2 8922 5274
anne-marie.allgrove@bakermckenzie.com

Patrick Fair
Sydney
Tel: +61 2 8922 5534
patrick.fair@bakermckenzie.com

Adrian Lawrence
Sydney
Tel: +61 2 8922 5204
adrian.lawrence@bakermckenzie.com

Ju Young Lee
Sydney
Tel: +61 2 8922 5260
juyoung.lee@bakermckenzie.com

Toby Patten
Melbourne
Tel: +61 3 9617 4456
toby.patten@bakermckenzie.com

Austria
Lukas Feiler
Vienna
Tel: +43 1 24250 450
lukas.feiler@bakermckenzie.com

Belgium
Elisabeth Dehareng
Brussels
Tel: +32 2 639 36 11
elisabeth.dehareng@bakermckenzie.com

Daniel Fesler
Brussels
Tel: +32 2 639 36 11
daniel.fesler@bakermckenzie.com

Brazil
Gabriela Paiva-Morette
Sao Paulo
Tel: +55 11 3048 6785
gabriela.paiva-morette@trenchrossi.com

Flavia Rebello
Sao Paulo
Tel: +55 11 3048 6851
flavia.rebello@trenchrossi.com

Canada
Andrew Chien
Toronto
Tel: +416 865 2315
andrew.chien@bakermckenzie.com

Theodore Ling
Toronto
Tel: +416 865 6954
theodore.ling@bakermckenzie.com

Jonathan Tam
Toronto
Tel: +416 865 2324
jonathan.tam@bakermckenzie.com

China (PRC)
Nancy Leigh
Hong Kong
Tel: +852 2846 1787
nancy.leigh@bakermckenzie.com
Zhenyu Ruan  
Shanghai  
Tel: +86 21 6105 8577  
zhenyu.ruan@bakermckenzie.com

Howard Wu  
Shanghai  
Tel: +86 21 6105 8538  
howard.wu@bakermckenzie.com

Colombia  
Sandra Castillo  
Bogota  
Tel: +57 1 634 1530  
sandra.castillo@bakermckenzie.com

Carolina Pardo  
Bogota  
Tel: +57 1 634 1559  
carolina.pardo@bakermckenzie.com

Czech Republic  
Jiri Cermak  
Prague  
Tel: +420 236 045 001  
jiri.cermak@bakermckenzie.com

Milena Hoffmanova  
Prague  
Tel: +420 236 045 001  
milena.hoffmanova@bakermckenzie.com

Denmark  
Lisa Bo Larsen  
Copenhagen  
Tel: +45 38 77 45 68  
lbl@kromannreumert.com

Daiga Grunte-Sonne  
Copenhagen  
Tel: +45 38 77 41 18  
DSO@kromannreumert.com

Finland  
Hannu Järvinen  
Helsinki  
Tel: +358 40 550 0306  
hannu.jarvinen@borenius.com

Susanna Karlsson  
Helsinki  
Tel: + 358 20 713 3298  
susanna.karlsson@borenius.com

France  
Magalie Dansac  
Paris  
Tel: +33 1 44 17 59 82  
Magalie.dansac@bakermckenzie.com

Denise Lebeau-Marianna  
Paris  
Tel: +33 1 44 17 53 33  
denise.lebeau-marianna@bakermckenzie.com

Germany  
Wolfgang Fritzemeyer  
Munich  
Tel: +49 89 55238 154  
wolfgang.fritzemeyer@bakermckenzie.com

Holger Lutz  
Frankfurt  
Tel: +49 69 29908 638  
holger.lutz@bakermckenzie.com

Michael Schmid  
Munich  
Tel: +49 89 55238 211  
michael.schmid@bakermckenzie.com

Matthias Scholz  
Frankfurt  
Tel: +49 69 29908 203  
matthias.scholz@bakermckenzie.com

Julia Wendler  
Munich  
Tel: +49 89 55238 261  
 julia.wendler@bakermckenzie.com

Greece  
Vassilis Constantes  
Athens  
Tel: +30 210 720 6900  
v.constantes@vplaw.gr
Daisuke Tatsuno  
Tokyo  
Tel: +813 6271 9479  
daisuke.tatsuno@bakermckenzie.com

Luxembourg

Audrey Rustichelli  
Luxembourg  
Tel: +352 261844 249  
audrey.rustichelli@bakermckenzie.com

Salome Steinberger  
Luxembourg  
Tel: +352 261844 257  
salome.steinberger@bakermckenzie.com

Malaysia

Shameen Binti Mohd. Haaziq Pillay  
Kuala Lumpur  
Tel: +603 2298 7943  
Shameen.mohd.haaziqPillay@WongPartners.com

Woo Wei Kwang  
Kuala Lumpur  
Tel: +603 2298 7898  
weikwang.woo@WongPartners.com

Mexico

Sergio Legorreta-Gonzalez  
Mexico City  
Tel: +52 55 5279 2954  
sergio.legorreta-gonzalez@bakermckenzie.com

Carlos Vela-Trevino  
Mexico City  
Tel: +52 55 5279 2911  
carlos.vela-trevino@bakermckenzie.com

Netherlands

Silvia van Schaik  
Amsterdam  
Tel: +31 20 551 7146  
silvia.vanschaik@bakermckenzie.com

Wouter Seinen  
Amsterdam  
Tel: +31 20 551 7161  
wouter.seinen@bakermckenzie.com

New Zealand

Carl Blake  
Auckland  
Tel: +64 9 977 5163  
carl.blake@simpsongrierson.com

Karen Ngan  
Auckland  
Tel: +64 9 977 5080  
karen.ngan@simpsongrierson.com

Norway

Cato Lower  
Oslo  
Tel: +47 98 29 45 15  
clo@adeb.no

Espen Sandvik  
Oslo  
Tel: +47 98 29 45 41  
esa@adeb.no

Peru

Viviana Chavez  
Lima  
Tel: +51 1 618 8500 Ext. 421  
Viviana.chavez@bakermckenzie.com

Javier Tovar  
Lima  
Tel: +51 1 618 8500 Ext. 550  
javier.tovar@bakermckenzie.com

Teresa Tovar  
Lima  
Tel: +51 1 618 8500 Ext. 552  
Teresa.tovar@bakermckenzie.com

Philippines

Bienvenido Marquez  
Manila  
Tel: +63 2 819 4936  
bienvenido.marquez@quisumbingtorres.com

Divina Ilas-Panganiban  
Manila  
Tel: +63 2 819 4961  
divina.ilas-panganiban@quisumbingtorres.com
Poland

**Magdalena Kogut-Czarkowska**
Warsaw
Tel: +48 22 445 3452
magdalena.kogut-czarkowska@bakermckenzie.com

**Radosław Nożykowski**
Warsaw
Tel: +48 22 445 3210
radoslaw.nozykowski@bakermckenzie.com

Portugal

**César Bessa Monteiro**
Lisbon
Tel: +351 213 264 747
cesar.bmonteiro@pbbr.pt

**Ricardo Henriques**
Lisbon
Tel: +351 213 264 747
ricardo.henriques@pbbr.pt

Russia

**Edward Bekeschenko**
Moscow
Tel: +7 495 787 2700
edward.bekeschenko@bakermckenzie.com

**Dmitry Lysenko**
Moscow
Tel: +7 495 787 2700
dmitry.lysenko@bakermckenzie.com

**Vadim Perevalov**
Moscow
Tel: +7 495 787 2700
vadim.perevalov@bakermckenzie.com

**Ekaterina Sorokina**
Moscow
Tel: +7 495 787 2700
Ekaterina.sorokina@bakermckenzie.com

Saudi Arabia

**Judes Abboud**
Dubai
Tel: + 971 442 30080
judes.abboud@bakermckenzie.com

**Haifa Bahaian**
Riyadh
Tel: + 966 11 265 8900, Ext. 8968
haifa.bahaian@bakermckenzie.com

**Aisha Gondal**
Riyadh
Tel: + 966 11 265 8900, Ext. 8913
aisha.gondal@bakermckenzie.com

**George Sayen**
Riyadh
Tel: + 966 11 265 8900, Ext. 8911
gorge.sayen@bakermckenzie.com

Singapore

**Ken Chia**
Singapore
Tel: +65 6434 2558
ken.chia@bakermckenzie.com

South Africa

**Darryl Bernstein**
Johannesburg
Tel: +27 0 11 911 4367
darryl.bernstein@bakermckenzie.com

**Widaad Ebrahim**
Johannesburg
Tel: +27 0 11 911 4384
widaad.ebrahim@bakermckenzie.com

**Deepa Ramjee**
Johannesburg
Tel: +27 0 11 911 4368
deepa.ramjee@bakermckenzie.com

South Korea

**Boseong Kim**
Seoul
Tel: +82 2 721 4130
boskim@kcllaw.com
Junghwa Lee
Seoul Tel: +82 2 721 4147
jhlee@kcllaw.com

Spain

Rosario Alvarez
Madrid
Tel: +34 91 230 4513
Rosario.Alvarez@bakermckenzie.com

Jordi Masdevall
Barcelona
Tel: +34 93 206 0820
jordi.masdevall@bakermckenzie.com

Raul Rubio
Madrid
Tel: +34 91 436 6639
raul.rubio@bakermckenzie.com

Sweden

Sten Bauer
Stockholm
Tel: +46 (0) 8 566 177 16
sten.bauer@bakermckenzie.com

Johan Strand
Stockholm
Tel: +46 (0) 8 566 177 41
johan.strand@bakermckenzie.com

Switzerland

Nicolas Passadelis
Zurich
Tel: +41 44 384 1209
nicolas.passadelis@bakermckenzie.com

Taiwan

H. Henry Chang
Taipei
Tel: +886 2 2715 7259
henry.chang@bakermckenzie.com

Chris Tsai
Taipei
Tel: +886 2 2715 7310
chris.tsai@bakermckenzie.com

Thailand

Pattaraphan Paiboon
Bangkok
Tel: +66 02 636 2000 Ext. 4568
pattaraphan.paiboon@bakermckenzie.com

Dhiraphol Suwanprateep
Bangkok
Tel: +66 02 636 2000 Ext. 4950
dhiraphol.suwanprateep@bakermckenzie.com

Ukraine

Oleksiy Stolyarenko
Kyiv
Tel: +380 44 590 0101
oleksiy.stolyarenko@bakermckenzie.com

United Kingdom

Robbie Downing
London
Tel: +44 20 7919 1161
robbie.downing@bakermckenzie.com

Dyann-Heward Mills
London
Tel: +44 20 7919 1269
dyann.heward-mills@bakermckenzie.com

Benjamin Slinn
London
Tel: +44 20 7919 1783
benjamin.slinn@bakermckenzie.com

United States

Amy de La Lama
Chicago
Tel: +1 312 861 2923
amy.delalama@bakermckenzie.com

Lothar Determann
Palo Alto
Tel: +1 650 856 5533
lothar.determann@bakermckenzie.com
Global Data Breach Notification Guide

Jeff Dunifon
New York
Tel: +1 212 626 4323
jeff.dunifon@bakermckenzie.com

Michael Egan
Washington, D.C.
Tel: +1 202 452 7022
michael.egan@bakermckenzie.com

Brian Hengesbaugh
Chicago
Tel: +1 312 861 3077
brian.hengesbaugh@bakermckenzie.com

Heather Mantegna Fitzwater
Chicago
Tel: +1 312 861 8808
heather.mantegna@bakermckenzie.com

Lindsay Martin
Chicago
Tel: +1 312 861 2949
lindsay.martin@bakermckenzie.com

Brandon Moseberry
Chicago
Tel: +1 312 861 8265
brandon.moseberry@bakermckenzie.com

Michael Stoker
Chicago
Tel: +1 312 861 2870
michael.stoker@bakermckenzie.com

Uruguay

Santiago Dutra
Montevideo
Tel: +598 2900 1000 ext. 1610
sdutra@ferrere.com

Martin Pesce
Montevideo
Tel: +598 2900 1000 ext. 7982
mpesce@ferrere.com

Vietnam

Yee Chung Seck
Ho Chi Minh City
Tel: +84 8 829 6234
yeechung.seck@bakermckenzie.com

Minh Tri Quach
Hanoi
Tel: +84 4 3936 9605
minhtri.quach@bmvn.com.vn
# Table of Contents

Editors’ Note .................................................................................................................. i
Baker & McKenzie’s Global IT/C Data Security Leadership Team .................. iii
Contributing Lawyers ................................................................................................. vi
Argentina .................................................................................................................. 1
Australia ................................................................................................................... 5
Austria ........................................................................................................................ 9
Belgium ...................................................................................................................... 13
Brazil .......................................................................................................................... 24
Canada ....................................................................................................................... 28
China .......................................................................................................................... 36
Colombia .................................................................................................................... 40
Czech Republic .......................................................................................................... 44
Denmark ..................................................................................................................... 48
Finland ....................................................................................................................... 54
France ........................................................................................................................ 60
Germany ..................................................................................................................... 64
Greece ......................................................................................................................... 74
Hong Kong ................................................................................................................. 78
Hungary ...................................................................................................................... 82
Iceland ........................................................................................................................ 88
India ............................................................................................................................ 92
Indonesia ................................................................................................................... 96
Ireland ....................................................................................................................... 100
Israel ........................................................................................................................... 104
Italy ............................................................................................................................. 108
Japan .......................................................................................................................... 112
Luxembourg ............................................................................................................ 116
Malaysia ................................................................................................................... 122
Mexico .......................................................... 126
Netherlands .................................................. 130
New Zealand ................................................. 140
Norway .......................................................... 144
Peru .............................................................. 148
Philippines ..................................................... 152
Poland .......................................................... 156
Portugal ......................................................... 160
Russia ........................................................... 164
Saudi Arabia .................................................. 168
Singapore ...................................................... 170
South Africa ................................................... 175
South Korea ................................................... 181
Spain ............................................................ 187
Sweden ........................................................ 193
Switzerland ..................................................... 199
Taiwan .......................................................... 203
Thailand ......................................................... 207
Turkey .......................................................... 211
Ukraine .......................................................... 215
United Kingdom ............................................. 219
United States .................................................. 225
Uruguay .......................................................... 238
Vietnam ........................................................ 242
Baker & McKenzie Offices Worldwide ................... 246
Argentina

Guillermo Cervio
Buenos Aires
Tel: +54 11 4310 2223
guillermo.cervio@bakermckenzie.com

Roberto Grané
Buenos Aires
Tel: +54 11 4310 2214
roberto.grane@bakermckenzie.com
1. In your jurisdiction, are there legal requirements for organizations to provide notice of a breach of security for personal data or other company information?

No.

2. For each law and regulation identified in Question 1, please describe:

a. **The general scope of the breach notice requirement.**
   There is no specific mandatory obligation under the currently applicable regulations that require private sector companies to provide notice of a breach of security for personal data to affected individuals and/or governmental authorities. Nevertheless, companies affected by a security breach usually consider reporting the incident to their customers as best practice in order to allow them to adopt the appropriate course of action to protect their information and minimize damages. In addition, where the incident affects information related to any password or similar private information used by its employees, the company should report the incident to the affected employees to allow them to adopt the appropriate course of action (e.g., to change passwords).

b. **The definition or standard of a covered “data breach.”**
   Not applicable.

c. **Whether it is mandatory to notify affected individuals.**
   No.

d. **Whether it is mandatory to notify any government authorities.**
   No.

e. **Whether any other parties may need to be notified of the incident.**
   No.

f. **Whether the above rules are different if the company is acting as a data processor/service provider, and not acting as the data controller/owner of the information at issue.**
   No.
g. What are the potential penalties for non-compliance with the breach notice obligation?

None. Penalties, however, will relate to non-compliance with security measures. In this regard, the Authority may impose the following administrative sanctions:

(i) warnings;
(ii) suspension;
(iii) fines; and
(iv) closure or cancellation of the file, register or databases.
Australia

Ann-Marie Allgrove
Sydney
Tel: +61 2 8922 5274
anne-marie.allgrove@bakermckenzie.com

Toby Patten
Melbourne
Tel: +61 3 9617 4456
toby.patten@bakermckenzie.com

Patrick Fair
Sydney
Tel: +61 2 8922 5534
patrick.fair@bakermckenzie.com

Ju Young Lee
Sydney
Tel: +61 2 8922 5260
juyoung.lee@bakermckenzie.com

Adrian Lawrence
Sydney
Tel: +61 2 8922 5204
adrian.lawrence@bakermckenzie.com
1. In your jurisdiction, are there legal requirements for organizations to provide notice of a breach of security for personal data or other company information?

No.

While Australia does not have a mandatory data breach notification law, the Office of the Australian Information Commission provides for a voluntary data breach notification scheme.

2. For each law and regulation identified in Question 1, please describe:

a. The general scope of the breach notice requirement.
   The voluntary data breach notification applies to all personal information and all industries.

b. The definition or standard of a covered “data breach.”
   Notification is recommended if the data breach creates a real risk of serious harm to the individual.

c. Whether it is mandatory to notify affected individuals.
   No. However, the scheme recommends that individuals be notified as soon as possible, with information regarding a description of the breach, type of personal information involved, steps to help mitigate, and contact details for information and assistance.

d. Whether it is mandatory to notify any government authorities.
   No.

   However, the scheme recommends considering whether the regulator, law enforcement, professional or regulatory bodies or other bodies should be notified.

e. Whether any other parties may need to be notified of the incident.
   No.

f. Whether the above rules are different if the company is acting as a data processor/service provider, and not acting as the data controller/owner of the information at issue.
   No.
g. What are the potential penalties for non-compliance with the breach notice obligation?

No penalties as this is a voluntary scheme.
Austria

Lukas Feiler
Vienna
Tel: +43 1 24250 450
lukas.feiler@bakermckenzie.com
1. In your jurisdiction, are there legal requirements for organizations to provide notice of a breach of security for personal data or other company information?

Yes.

**Please identify the name of the relevant law(s) or regulation(s).**

Law.

The relevant laws are (i) 24(2a) of the Austrian Data Protection Act 2000 and (ii) 95a of the Austrian Telecommunications Act 2003.

2. For each law and regulation identified in Question 1, please describe:

a. **The general scope of the breach notice requirement.**

The Data Protection Act 2000 requires a data controller to inform data subjects about any systematic and serious illegal use of their personal data if there is a risk of harm to the data subjects.

The Telecommunications Act 2003 provides a sector-specific breach notification requirement for providers of publicly available electronic communications services (e.g., telephone network operators and Internet access providers). These providers have to notify the Austrian Data Protection Authority of any breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data.

In addition, the data subjects have to be notified if the breach is likely to adversely affect their privacy or personal data. Also, under general principles of Austrian contract law, one contracting party has the implied obligation to protect the other contracting party from any harm in connection with the performance of the contract. Thus, unless otherwise agreed, each contracting party has a general obligation to notify the other party of security breaches to the extent that such notification may protect the other party from further harm.

b. **The definition or standard of a covered “data breach.”**

The notification trigger under the Data Protection Act 2000 is a systematic and serious illegal use of personal data. There is no case law regarding the interpretation of this trigger and these terms are also not defined in the statute itself. In any case, a notification is not required if there is only insignificant harm to be expected and the costs of informing all data subjects concerned would result in a disproportionate effort.

The notification trigger under the Telecommunications Act 2003 is a breach of security leading to the accidental or unlawful destruction, loss, alteration,
unauthorized disclosure of, or access to, personal data. However, there is no notification requirement if the provider has demonstrated to the satisfaction of the Austrian Data Protection Authority that it has implemented appropriate security measures (e.g., strong encryption) and has applied these measures to the data concerned.

c. **Whether it is mandatory to notify affected individuals.**
   Yes.

The Data Protection Act 2000 stipulates a breach notification has to be performed without undue delay. The content of the notification has to include the data controller’s identity and his data protection register number.

The Telecommunications Act 2003 requires the provider to notify the data subjects without undue delay. The notification to the data subjects has to contain information on:

(i) the nature of the personal data breach,
(ii) the contact points where more information can be obtained, and
(iii) recommended measures to mitigate the possible adverse effects of the personal data breach.

d. **Whether it is mandatory to notify any government authorities.**
   Yes (under Telecommunications Act 2003).

The Telecommunications Act 2003 requires the provider to notify the Austrian Data Protection Authority of any personal data breach without undue delay. The notification to the Data Protection Authority has to contain information on:

(i) the nature of the personal data breach,
(ii) the contact points where more information can be obtained,
(iii) recommended measures to mitigate the possible adverse effects of the personal data breach, and
(iv) a description of the consequences of, and the measures proposed or taken by the provider to address the personal data breach.

e. **Whether any other parties may need to be notified of the incident.**
   No.

f. **Whether the above rules are different if the company is acting as a data processor/service provider, and not acting as the data controller/owner of the information at issue.**
   Yes.
The Data Protection Act 2000 does not impose any notification requirements on data processors.

The Telecommunications Act 2003 applies irrespective of whether the provider acts as a controller or as a processor.

g. **What are the potential penalties for non-compliance with the breach notice obligation?**

The Data Protection Act 2000 provides an administrative fine of up to EUR 25,000 in case of non-compliance with the notification requirement. The Telecommunications Act 2003 provides an administrative fine of up to EUR 58,000.
Belgium

Daniel Fesler
Brussels
Tel: +32 2 639 36 11
daniel.fesler@bakermckenzie.com

Elisabeth Dehareng
Brussels
Tel: +32 2 639 36 11
elisabeth.dehareng@bakermckenzie.com
1. In your jurisdiction, are there legal requirements for organizations to provide notice of a breach of security for personal data or other company information?

Yes, in Belgium there are legal requirements for organizations to provide notice of a breach of security for personal data or other company information.

Please identify the name of the relevant law(s) or regulation(s).

Law.


iii. *Article 30 of the Belgian Criminal Investigation Code*

iv. *Belgian Data Protection Act of December 8, 1992*

v. *Belgian civil law principles of good faith and fairness and general duty of care sanctioned by Article 1382 of the Belgian Civil Code (Belgian law on torts)* (and Articles 1146 & seq. of the same code for contractual matters)

vi. *Voluntary notification of data breaches as per the Privacy Commission’s protocol and guidelines*

2. For each law and regulation identified in Question 1, please describe:

a. The general scope of the breach notice requirement.


A limited notification obligation applies to providers of electronic communication services (e.g., telecom operators, mobile phone communication services providers, internet access providers, etc.).


Transport, caching and hosting services providers.

(iii) *Article 30 of the Belgian Criminal Investigation Code*

Applies to anyone.
(iv) **Belgian Data Protection Act of December 8, 1992**

Applies to data controllers.

(v) **Belgian civil law principles of good faith and fairness and general duty of care sanctioned by Article 1382 of the Belgian Civil Code (Belgian law on torts) (and Articles 1146 & seq. of the same code for contractual matters)**

In accordance with the Belgian civil law principles of good faith and fairness in contractual relationships, as well as the general duty of care sanctioned by Article 1382 and seq. of the Belgian Civil Code (and Articles 1146 & seq. of the same code for contractual matters), a data controller should inform its customers or other persons affected (or even the public at large, e.g., for the sake of reaching a large audience when it is not possible to identify precisely the persons affected), and/or authorities, where such information could help in mitigating the prejudice suffered by customers or third parties, if any.

This notification duty is not limited to personal data and could apply to any type of data or of customers (such as data pertaining to legal entities).

(vi) **Voluntary notification of data breaches as per the Privacy Commission’s protocol and guidelines**

This is a voluntary protocol that applies to data controllers.

**b. The definition or standard of a covered “data breach.”**


In case of a security breach affecting an electronic communications service accessible to the public, providers of electronic communication services should notify the Belgian Privacy Commission without undue delay.


Transport, caching and hosting services providers have the obligation to report to the public prosecutor alleged illegal activities on their systems that they become aware of; this may then apply to unauthorized access and/or use to data they are transporting, caching or hosting.

(iii) **Article 30 of the Belgian Criminal Investigation Code**

Anyone who takes knowledge of a hacking consisting in – or being part of – an attempt to harm people or steal someone’s property.
(iv) **Belgian Data Protection Act of December 8, 1992**

Falls within the scope of the data controller’s general loyalty obligation set forth by Article 4 of the Belgian Data Protection Act (the “DPA”), combined with the obligation to inform data subjects about the recipient(s) of their data (Article 9 of the DPA) in case the breach results from an action of the data controller, whether such action is voluntary or not.

(v) **Belgian civil law principles of good faith and fairness and general duty of care sanctioned by Article 1382 of the Belgian Civil Code (Belgian law on torts) (and Articles 1146 & seq. of the same code for contractual matters)**

Companies should report a breach where such information could help mitigating the prejudice suffered by customers or third parties, if any.

(vi) **Voluntary notification of data breaches as per the Privacy Commission’s protocol and guidelines**

First, such guidelines require the data controller to inform the Privacy Commission within 48 hours of the discovery of the data breach, and of its cause(s) and impact. A notification form is available on the Belgian Privacy Commission’s website; the notification can be completed in two steps: first, a preliminary form can be filed electronically including a description of the breach, the types of data affected, the possible causes of the breach and the preliminary measures taken to mitigate the risk such as information of data subject, and, in a second stage once the breach has been investigated, a full notification.

However, pursuant to the Privacy Commission’s guidance provided on its website, no such notification is necessary where:

- the data breach does not prejudice the data subjects’ private life or personal data; or
- the data were encrypted or secured in such a way that data are incomprehensible to third parties (provided that the security key has not also been leaked); or
- the data subjects concerned are immediately informed of the nature and consequences of the data breach, provided that less than 100 data subjects are affected by such data breach and that no sensitive or financial data are concerned.

Secondly, the Privacy Commission’s protocol also requires the data controller to notify data subjects of data breaches by a communication method that guarantees quick receipt of such information, unless (i) the data were encrypted or secured in such a way that data are incomprehensible to third parties, or (ii) in exceptional cases where the notification would risk harming...
the efficient conduct of an investigation (in which case such notification would however only be delayed).

The above Privacy Commission’s recommendation is, in any case, not mandatory except if the data breach at stake can be considered as resulting from the use of personal data, by or on behalf of the data controller, for a purpose that was not previously notified to the data subjects, in which case the Data Protection Act makes it mandatory for the data controller to inform data subjects of such new use or new purpose. This may happen, for instance, where the data controller publishes, even by accident, personal data that should have been kept confidential. See Section iv of this document for more details.

c. Whether it is mandatory to notify affected individuals.

Yes (subject to certain conditions). When the personal data breach is likely to adversely affect the personal data privacy of a subscriber or individual, the provider shall notify the subscriber or individual without undue delay. The notification to the subscriber or individual shall at least describe the nature of the personal data breach and the contact points where more information can be obtained, and shall recommend measures to mitigate the possible adverse effects of the personal data breach.

Notification of a personal data breach to a subscriber or individual concerned shall not be required if the provider has demonstrated to the satisfaction of the competent authority that it has implemented appropriate technological protection measures, and that those measures were applied to the data concerned by the security breach. Such technological protection measures shall render the data unintelligible to any person who is not authorised to access it.

No.

(iii) Article 30 of the Belgian Criminal Investigation Code
No.

(iv) Belgian Data Protection Act of December 8, 1992
Yes, data controllers must inform data subjects about the processing of their data.
Belgian civil law principles of good faith and fairness and general duty of care sanctioned by Article 1382 of the Belgian Civil Code (Belgian law on torts) (and Articles 1146 & seq. of the same code for contractual matters)

Yes. Companies should inform the affected individuals, where such information could help in mitigating the prejudice suffered by customers or third parties if any.

The scope and timing of such information would mainly depend on what is necessary, in light of the circumstances of the case, to allow the affected individuals or third parties to take any appropriate measures to mitigate or to avoid their (potential) prejudice.

Voluntary notification of data breaches as per the Privacy Commission’s protocol and guidelines

No. This is a voluntary protocol, but, if followed, it will require notification to affected individuals. In any event, the obligation to notify individuals may derive from the other legal bases identified above.

d. Whether it is mandatory to notify any government authorities.


Yes. It is mandatory to notify the Belgian Privacy Commission. The notification shall describe the consequences of, and the measures proposed or taken by the provider to address, the personal data breach.


Yes, the public prosecutor must be notified.

(iii) Article 30 of the Belgian Criminal Investigation Code

Yes, the public prosecutor must be notified.

(iv) Belgian Data Protection Act of December 8, 1992

No (only a voluntary notification to the Belgian Privacy Commission exists).

(v) Belgian civil law principles of good faith and fairness and general duty of care sanctioned by Article 1382 of the Belgian Civil Code (Belgian law on torts) (and Articles 1146 & seq. of the same code for contractual matters)

Yes. Companies should inform the relevant government authorities, where such information could help in mitigating the prejudice suffered by customers or third parties if any.
The scope and timing of such information would mainly depend on what is necessary, in light of the circumstances of the case, to allow the affected individuals or third parties to take any appropriate measures to mitigate or to avoid their (potential) prejudice.

(vi) Voluntary notification of data breaches as per the Privacy Commission’s protocol and guidelines
No. This is a voluntary protocol, but if followed, it will require notification to the Belgian Privacy Commission under the guidelines described in section (b).

e. Whether any other parties may need to be notified of the incident.

No.

No.

(iii) Article 30 of the Belgian Criminal Investigation Code
No.

(iv) Belgian Data Protection Act of December 8, 1992
No.

(v) Belgian civil law principles of good faith and fairness and general duty of care sanctioned by Article 1382 of the Belgian Civil Code (Belgian law on torts) (and Articles 1146 & seq. of the same code for contractual matters)
Yes. As the case may arise, companies must inform the public at large for the sake of reaching a large audience when it is not possible to identify precisely the persons affected.

(vi) Voluntary notification of data breaches as per the Privacy Commission’s protocol and guidelines
No.
f. Whether the above rules are different if the company is acting as a data processor/service provider, and not acting as the data controller/owner of the information at issue.

No. The notification obligation applies to the providers of electronic communications, whether acting as controller or processor.

No. The notification obligation applies to the providers of transport, caching and hosting services, whether acting as controller or processor.

(iii) *Article 30 of the Belgian Criminal Investigation Code*
No.

(iv) *Belgian Data Protection Act of December 8, 1992*
Yes, this obligation only applies to data controllers.

(v) *Belgian civil law principles of good faith and fairness and general duty of care sanctioned by Article 1382 of the Belgian Civil Code (Belgian law on torts)* (and Articles 1146 & seq. of the same code for contractual matters)
No.

(vi) *Voluntary notification of data breaches as per the Privacy Commission’s protocol and guidelines*
Yes, only applies to data controllers.

g. What are the potential penalties for non-compliance with the breach notice obligation?

Failure to comply would result in liability in case such failure would contribute, directly or indirectly, in whole or in part, to harm to the affected individual.

Failure to comply would result in liability in case such failure would contribute, directly or indirectly, in whole or in part, to harm to the affected individual.
(iii) **Article 30 of the Belgian Criminal Investigation Code**

Failure to comply would result civil in liability in case such failure would contribute, directly or indirectly, in whole or in part, in harm to the affected individual. Such failure may also result in criminal liability if reporting to the public prosecutor could have helped to protect a person facing a clear and imminent serious hazard threatening her life or her physical or mental well-being (jail term from 8 days to 2 years, fine from € 300 to € 3,000) or could have prevented a person from being killed or harmed (jail term of 8 days to 2 years, fine from € 300 to € 6,000).

(iv) **Belgian Data Protection Act of December 8, 1992**

Failure to comply with the data controller’s obligations (including informing data subjects about the processing - including the purposes and recipients - of their personal data) under the Belgian Data Protection Act is criminally sanctioned with fines from € 600 to € 600,000.

In addition, Belgian courts may, as the case may arise, order publication of their decisions in whole or by excerpt in one or more newspapers, as well as the seizure of any privacy infringing equipment or data, and rectification or destruction of personal data; courts may also prohibit the controller from processing any personal data for up to 2 years.

Criminal and/or civil claims filed by individuals are also possible. A data controller is liable for any damage caused by an act in violation of the Data Protection Act, unless he can prove that he did not cause the damage.

(v) **Belgian civil law principles of good faith and fairness and general duty of care sanctioned by Article 1382 of the Belgian Civil Code (Belgian law on torts) (and Articles 1146 & seq. of the same code for contractual matters)**

Failure to comply with the general duty of care provisions or principles would result in liability in case such failure would contribute, directly or indirectly, in whole or in part, harm to the affected individual.

(vi) **Voluntary notification of data breaches as per the Privacy Commission’s protocol and guidelines**

Although the Belgian Privacy Commission has no power to impose sanctions (yet), the Privacy Commission indicated, in its above-mentioned Recommendation of 2013 regarding security breaches, that, in case of non-compliance with its recommendations, it would use all legal means to engage the responsibility of the data controllers, including through criminal prosecution by referring the case to the public prosecutor.

**General Note:** Please note that new breach notification duties will be set forth under the General Data Protection Regulation and the Network Information Security Directive once implemented into Belgian law. The General Data
Protection Regulation is set to become applicable on the 25th of May 2018. The Network and Information Security Directive ("NIS Directive") is set to come into force on the 8th of August 2016. However, it is not immediately applicable since each Member State then has until the 9th of May 2018 to implement the NIS Directive into its national legislation, with the mandate to apply the NIS Directive as of the 10th of May 2018.
Brazil

Flavia Rebello
Sao Paulo
Tel: +55 11 3048 6851
flavia.rebello@trenchrossi.com

Gabriela Paiva-Morette
Sao Paulo
Tel: +55 11 3048 6785
gabriela.paiva-morette@trenchrossi.com
1. In your jurisdiction, are there legal requirements for organizations to provide notice of a breach of security for personal data or other company information?

No.

There are no specific rules addressing data security breaches. However, as data controllers are generally liable for any data security breach, it is highly advisable to inform the affected data subjects and the relevant bodies as soon as the data controller becomes aware of a data security breach. In cases of breach of personal data of consumers, for instance, we do recommend that consumer authorities be notified of said breach.

This is especially important in situations where an early notice can be helpful to mitigate possible damages to the data subjects (e.g., by allowing the data subjects to change passwords or take other precautionary measures to avoid damages). Accordingly, the data controllers may also be able to reduce their liability for damages that can be mitigated by means of an early notification of the security breach.

2. For each law and regulation identified in Question 1, please describe:

a. The general scope of the breach notice requirement.

Not applicable.

b. The definition or standard of a covered “data breach.”

Not applicable.

c. Whether it is mandatory to notify affected individuals.

Not applicable.

d. Whether it is mandatory to notify any government authorities.

Not applicable.

e. Whether any other parties may need to be notified of the incident.

Not applicable.

f. Whether the above rules are different if the company is acting as a data processor/service provider, and not acting as the data controller/owner of the information at issue.

Not applicable.
g. What are the potential penalties for non-compliance with the breach notice obligation?

An organization that is involved in a data breach situation may be subject to an administrative fine, penalty or sanction, or civil actions and/or class actions. However, neither the Internet Legal Framework nor any other Brazilian law regulates the applicable procedure for such cases.
Canada

Theodore Ling
Toronto
Tel: +416 865 6954
theodore.ling@bakermckenzie.com

Jonathan Tam
Toronto
Tel: +416 865 2324
jonathan.tam@bakermckenzie.com

Andrew Chien
Toronto
Tel: +416 865 2315
andrew.chien@bakermckenzie.com
1. In your jurisdiction, are there legal requirements for organizations to provide notice of a breach of security for personal data or other company information?

Yes.

Please identify the name of the relevant law(s) or regulation(s).

**Canada**: Personal Information Protection and Electronic Documents Act, SC 2000, c 5.*  
*Mandatory data breach notification obligation yet to be declared in force.

**Alberta**: Personal Information Protection Act, SA 2003, c P-6.5; Personal Information Protection Act Regulation, Alta Reg 366/2003.

**Manitoba**: The Personal Information Protection and Identity Theft Prevention Act, CCSM, c P33.7.*  
*Law yet to be declared in force.


**Newfoundland and Labrador**: Personal Health Information Act, SNL 2008, c P-7.01; Personal Health Information Regulations, NLR 38/11.

**New Brunswick**: Personal Health Information Privacy and Access Act, SNB 2009, c P-7.05; Provincial Offences Procedure Act, SNB 1987, c P-22.1.

**Nova Scotia**: Personal Health Information Act, SNS 2010, c 41.

2. For each law and regulation identified in Question 1, please describe:

a. The general scope of the breach notice requirement.

**Canada**: Canada’s federal privacy law was recently amended to include a mandatory data breach notice requirement. These amendments have received royal assent and will be proclaimed into force on an unspecified date in the future. Under the amended law, organizations with control over personal information will be required to provide notification when there is a breach of security safeguards in respect of personal information and it is reasonable in the circumstances to believe that the breach creates a real risk of significant harm to an individual.

**Alberta**: Alberta’s privacy law requires any organization with personal information under its control to provide notice whenever there is a loss of, unauthorized access to, or disclosure of personal information, such that a
reasonable person would consider there to be a real risk of significant harm to an individual.

**Manitoba**: Manitoba recently enacted privacy legislation that has received royal assent but has not yet come into force. It is unclear when the law will be declared in force. Under this legislation, notification is generally required if an individual’s personal information under the custody or control of an organization is stolen, lost, or accessed in an unauthorized manner.

**Ontario**: Under Ontario’s health privacy law, a health information custodian is subject to a breach notification requirement where personal health information under its custody or control is stolen, lost, or accessed by unauthorized persons.

A bill is currently being debated in Ontario’s legislature which would, if passed, also require notification in the event that personal health information provided for the purpose of creating or maintaining an electronic health record is stolen, lost, accessed by unauthorized persons, or dealt with in a way that is not in accordance with Ontario’s health privacy law.

**Newfoundland and Labrador**: Under Newfoundland and Labrador’s health privacy law, a health custodian that has custody or control of personal health information is generally required to issue a breach notification where the information is stolen, lost, disposed of in a non-compliant manner, or disclosed to or accessed by an unauthorized person.

Additionally, the custodian must inform the Information and Privacy Commissioner of Newfoundland and Labrador if there is a “material breach” (as defined in the law) involving the unauthorized collection, use, or disclosure of personal health information.

The Commissioner may also recommend that a custodian notify the individual who is the subject of any information breach, even if the notification requirements are not triggered.

**New Brunswick**: Under New Brunswick’s health privacy law, a health custodian that has custody or control of personal health information is generally required to issue a breach notification where the information is stolen, lost, disposed of in a non-compliant manner, or disclosed to or accessed by an unauthorized person.

**Nova Scotia**: Under Nova Scotia’s health privacy law, a health custodian that has custody or control of personal health information is generally required to issue a breach notification where the custodian believes on a reasonable basis that the information is stolen, lost, or subject to unauthorized access, use, disclosure, copying, or modification.
b. The definition or standard of a covered “data breach.”

Canada: The data breach notification requirements under Canada’s federal privacy law (which are not yet in force) will apply where there is: (i) a breach of security safeguards; and (ii) a real risk of significant harm to an individual.

“Breach of security safeguards” means the loss of, unauthorized access to, or unauthorized disclosure of personal information. Canada’s federal privacy law defines “significant harm” to include “bodily harm, humiliation, damage to reputation or relationships, loss of employment, business or professional opportunities, financial loss, identity theft, negative effects on the credit record and damage to or loss of property.” Additionally, three factors have been set out to determine whether or not there is a real risk of significant harm to the individual, including: the sensitivity of the personal information involved in the breach; the probability that the personal information will be subject to misuse; and any other prescribed factor (currently, there are none).

Alberta: In Alberta, “significant harm” is a prerequisite for triggering the breach notification requirements, but it remains undefined in Alberta’s privacy law. However, the Office of the Information and Privacy Commissioner of Alberta has determined that for the harm to be significant, it must be “important, meaningful and more than trivial consequences or effects.”

Manitoba: Manitoba’s requirements (which are not yet in force) will not apply if the organization is instructed by a law enforcement agency to refrain from providing notification, or if the organization is satisfied that it is not reasonably possible for the personal information to be used unlawfully.

Ontario, Newfoundland and Labrador, New Brunswick, and Nova Scotia: The scope and limitations of the notification requirements for “data breaches” are generally the same under the health privacy laws of these four provinces.

Data breach notification requirements under the health privacy laws of these four provinces are generally triggered where personal health information is stolen, lost, or accessed by unauthorized persons. Personal health information has been defined to include information about an individual generally relating to his/her health and the provision of health care to that individual, among other things.

Specific Exceptions: There is an exception to the notification requirements in the health privacy laws of Ontario, Newfoundland and Labrador, and Nova Scotia, where the health information custodian is a researcher receiving personal health information from another health information custodian and other additional requirements are satisfied.

Furthermore, neither Newfoundland and Labrador nor New Brunswick requires notification if the custodian reasonably believes that the breach will not have an adverse impact upon (i) the provision of health care or other
benefits to the individual; (ii) the mental, physical, economic, or social well-being of the individual; or (iii) in the case of Newfoundland and Labrador, the breach does not lead to the identification of the individual.

c. Whether it is mandatory to notify affected individuals.

Canada: Once the relevant provisions in Canada’s federal privacy law are declared in force, a breach notification will need to be provided as soon as feasible after the organization determines that the breach has occurred. Regulations prescribing the form and manner of notifications have not yet been promulgated.

With respect to content, the notification will also need to contain sufficient information to allow the individual to understand the significance of the breach and to take steps to reduce the risk of harm that could result from it.

Alberta: While breaches do not automatically require notification of affected individuals by an organization, the Commissioner of Privacy for Alberta has the power to require organizations to notify individuals for whom there is a real risk of significant harm. There is no timing requirement for the notification, but it must be given directly to the individual (unless the Commissioner determines otherwise), and must include: (i) a description of the circumstances of the breach; (ii) the date or time period of the breach; (iii) a description of the personal information involved; (iv) a description of any steps the organization has taken to reduce the risk of harm; and (v) the contact information of a person who can answer questions about the breach on behalf of the organization.

Manitoba: Notification under Manitoba’s new legislation (which has yet to be declared in force) must be provided as soon as reasonably practicable. Regulations prescribing the form, manner, and content of notifications have not yet been promulgated.

Ontario, Newfoundland and Labrador, New Brunswick, and Nova Scotia: Under the health privacy laws of these provinces, custodians must notify individuals at the first reasonable opportunity if there is a breach regarding personal health information. There are no content requirements for the notification.

d. Whether it is mandatory to notify any government authorities.

Canada: Once the relevant provisions in Canada’s federal privacy law are declared in force, notification will need to be given to the Privacy Commissioner of Canada whenever a reportable breach is found. The timing and content of the notification follow the same standard as when the breach is reported to an affected individual.
**Alberta:** Organizations subject to the mandatory data breach notification requirements under Alberta’s privacy law must provide notice to the Commissioner of Privacy for Alberta without unreasonable delay. The notification must be in writing and contain: (i) a description of the circumstances of the breach; (ii) the date or time period of the breach; (iii) a description of the personal information involved; (iv) an assessment of the risk of harm to individuals due to the breach; (v) an estimate of the number of individuals to whom there is a real risk of significant harm; (vi) a description of any steps the organization has taken to reduce the risk of harm; (vii) a description of any steps the organization has taken to notify individuals of the breach; and (viii) the contact information of a person who can answer questions about the breach on behalf of the organization.

**Ontario:** Bill 78 is a proposed amendment to Ontario’s current health privacy law. If passed, the amended law would require personal health information custodians to immediately notify the Information and Privacy Commissioner of Ontario of any situations in which personal health information under their custody or control has been viewed, handled, made available, released, or dealt with in a way that does not accord with Bill 78 or its regulations (currently, there are none).

**Newfoundland and Labrador:** Personal health information custodians must provide notice to the Information and Privacy Commissioner of Newfoundland and Labrador when there is a “material breach”. The factors that are applied to determine if a breach is material are: (i) the sensitivity of the personal health information involved; (ii) the number of people whose personal health information was involved; (iii) whether the custodian reasonably believes that the personal health information involved has been or will be misused; and (iv) whether the cause of the breach or the pattern of breaches indicates a systemic problem. There are no timing or content requirements for this notification.

**Nova Scotia:** If the custodian makes the decision not to notify an individual as outlined above, then the custodian must notify the Privacy Review Officer of Nova Scotia as soon as possible. There are no content requirements for this notification.

e. **Whether any other parties may need to be notified of the incident.**

**Canada:** Once the relevant provisions in Canada’s federal privacy law are declared in force, data breaches must be reported to other organizations, subject to prohibitive laws, if the notification to that organization might reduce the risk of significant harm to individuals.
f. Whether the above rules are different if the company is acting as a data processor/service provider, and not acting as the data controller/owner of the information at issue.

No.

g. What are the potential penalties for non-compliance with the breach notice obligation?

**Canada:** Non-compliance with the breach notification requirements (which are not yet in force) can result in a fine of up to $100,000 per violation.

**Alberta:** Non-compliance with the breach notification requirements can result in a fine of up to $100,000 for organizations.

**Manitoba:** Once the relevant provisions come into force, an individual will be able to commence an action in a court of competent jurisdiction against an organization for damages arising from its failure to provide an individual with notification of the data breach as required.

**Ontario, Newfoundland and Labrador, New Brunswick, and Nova Scotia:** Willfully obstructing the privacy commissioners or officers in each of these provinces may result in (i) a fine of up to $250,000 in Ontario; (ii) a fine of up to $10,000 or imprisonment for a term not exceeding 6 months, or both, in Newfoundland and Labrador; (iii) a fine of between $240 and $10,200 in New Brunswick; and (iv) a fine of up to $10,000 or imprisonment for six months, or both, in Nova Scotia.

Proposed amendments to Ontario’s privacy health law may increase the maximum fine for organizations up to $500,000.
China

Nancy Leigh  
Hong Kong  
Tel: +852 2846 1787  
nancy.leigh@bakermckenzie.com

Howard Wu  
Shanghai  
Tel: +86 21 6105 8538  
howard.wu@bakermckenzie.com

Zhenyu Ruan  
Shanghai  
Tel: +86 21 6105 8577  
zhenyu.ruan@bakermckenzie.com
1. In your jurisdiction, are there legal requirements for organizations to provide notice of a breach of security for personal data or other company information?

No.

There is currently no “data protection authority” in China. There is also no law or regulation that provides for a duty to notify data subjects in case of a data breach. There are, however, some industry specific regulations that impose special duties on certain types of data carriers, including telecommunications service providers as well as companies in the financial and securities industries.

2. For each law and regulation identified in Question 1, please describe:

a. **The general scope of the breach notice requirement.**

Even in the absence of an obligation to notify in case of a data breach, there are a number of “information safety/security” regulations, which were promulgated, not particularly for the protection of personal data, but more out of concern for preserving state secrets and preventing data loss and business disruption which are considered harmful to the “public interest” in general. In that regard, government organizations and sensitive industries are required to install security systems, take preventive measures, and when any “information safety/security incident” occurs, report in a timely manner to the authorities and take emergency measures.

b. **The definition or standard of a covered “data breach.”**

“Information safety incidents” is a very broad concept, and generally covers all malicious attacks, equipment malfunctions or natural disasters which result in a massive breakdown of an information system and/or data loss or theft (it is a broader concept than that of “security breach”). These regulations do not include specific requirements for notifying the affected individuals, as they were drafted mainly from the perspective of state supervision and maintenance of order, instead of mitigating the impact on individuals.

c. **Whether it is mandatory to notify affected individuals.**

No.

d. **Whether it is mandatory to notify any government authorities.**

No.
e. Whether any other parties may need to be notified of the incident.

No.

f. Whether the above rules are different if the company is acting as a data processor/service provider, and not acting as the data controller/owner of the information at issue.

No.

g. What are the potential penalties for non-compliance with the breach notice obligation?

Failure to comply with the notification requirements as discussed above may lead to investigations and queries from the relevant authority and ultimately result in the imposition of administrative penalties.
Colombia

**Carolina Pardo**
Bogota
Tel: +57 1 634 1559
carolina.pardo@bakermckenzie.com

**Sandra Castillo**
Bogota
Tel: +57 1 634 1530
sandra.castillo@bakermckenzie.com
1. In your jurisdiction, are there legal requirements for organizations to provide notice of a breach of security for personal data or other company information?

Yes.

Please identify the name of the relevant law(s) or regulation(s).


2. For each law and regulation identified in Question 1, please describe:

a. The general scope of the breach notice requirement.

Under Law 1581 of 2012 (Colombian Personal Data Protection Statute - Law 1581), data controllers and data processors are obliged to notify any data breach to the Deputy Superintendent for the Protection of Personal Data at the Superintendence of Industry and Commerce (Colombian Data Protection Authority “DPA”), regardless of the place where the breach occurred.

Article 17 (n) of the Law provides that Data Controllers must comply with the following duties, and other provisions contained in this law and in other laws ruling the activity: (...) (n) Inform the Data Protection Authority when there is a breach of the security codes and there are risks to the management of the information of Data Subjects and Article 18 (k) of Law 1581, provides that Data Processors must comply with the following duties, and other provisions contained in this law and in other laws ruling the activity: (...) (n) Inform the Superintendence of Industry and Commerce when there is a breach of the security codes and there are risks to the management of the information of Data Subjects.

b. The definition or standard of a covered “data breach.”

Notification requirement is triggered when there is a breach of the security codes and there are risks to the management of the information of Data Subjects.

It has not been defined what should be understood as a harm triggering the need for a notification. Accordingly, we strongly recommend the notification of the DPA of the data breach as soon as possible regardless of the level of harm that was caused by the breach.

c. Whether it is mandatory to notify affected individuals.

No.
d. Whether it is mandatory to notify any government authorities.

Yes.

The authority is the Deputy Superintendent for the Protection of Personal Data at the Superintendence of Industry and Commerce ("DPA"). Because the obligation to report data breaches to the DPA has not been further regulated, there are no specific statutory deadlines to be observed to notify the breach to the DPA. However, as per informal discussions we have had with DPA officers, in evaluating what measures to take and in determining whether or not to open an investigation derived from the reported breach, said entity will evaluate the diligence that the data controller and/or processor exercised in handling the breach, which includes whether the notification to the DPA was made as soon as possible after the breach has taken place.

e. Whether any other parties may need to be notified of the incident.

No.

f. Whether the above rules are different if the company is acting as a data processor/service provider, and not acting as the data controller/owner of the information at issue.

No.

g. What are the potential penalties for non-compliance with the breach notice obligation?

Law 1581 of 2012 contains an extensive and strict set of obligations for data controllers and processors. Violation may result in the imposition of penalties that could go as high as USD 460,000 (at 2016 exchange rates; these amounts are indexed annually) and could also imply criminal liability. Accordingly, we also recommend that after notifying the breach to the DPA, the reporting data controller and/or processor verifies compliance with the remaining obligations contained in Law 1581 of 2012 and Decree 1377 of 2013, as in light of the breach notification, it is likely that the DPA will open an investigation. Thus, it is in the reporting data controller’s and/or processor ‘s best interest to understand the obligations under the Law and Decree, determine to what extent it has complied or not with their requirements and take any required measures.
Czech Republic

Jiri Cermak
Prague
Tel: +420 236 045 001
jiri.cermak@bakermckenzie.com

Milena Hoffmanova
Prague
Tel: +420 236 045 001
milena.hoffmanova@bakermckenzie.com
1. In your jurisdiction, are there legal requirements for organizations to provide notice of a breach of security for personal data or other company information?

Yes.

**Please identify the name of the relevant law(s) or regulation(s).**

Act No. 127/2005 Coll., on Electronic Communications (“ECA”), as amended - Section 88

2. For each law and regulation identified in Question 1, please describe:

a. **The general scope of the breach notice requirement.**
   
The ECA privacy breach notice requirement applies only to organizations providing publicly available services of electronic communications.

b. **The definition or standard of a covered “data breach.”**
   
   For electronic communications providers, data breach pertains to any breach of protection of personal data of an individual.

c. **Whether it is mandatory to notify affected individuals.**
   
   For electronic communications providers, yes.

   Notifying affected individuals is required in case the data breach is capable of impacting the privacy of an individual in a particularly serious manner. Notification of an affected individual should be carried out without any delay.

   In addition to the duty to notify under the ECA, there is a general duty to prevent damage that may apply, meaning that any security breach that may cause damage to data subjects should be duly reported to them in order to allow such individuals to adopt the appropriate course of action (e.g., change of passwords, etc.).

d. **Whether it is mandatory to notify any government authorities.**
   
   For electronic communications providers, yes.

   Office for Personal Data Protection needs to be notified about such data breach without any delay.

e. **Whether any other parties may need to be notified of the incident.**
   
   No.
f. Whether the above rules are different if the company is acting as a data processor/service provider, and not acting as the data controller/owner of the information at issue.

No.

g. What are the potential penalties for non-compliance with the breach notice obligation?

The competent regulatory authority may impose a fine of up to the maximum amount of CZK 20 million.
Denmark

Lisa Bo Larsen
Copenhagen
Tel: +45 38 77 45 68
lbl@kromannreumert.com

Daiga Grunte-Sonne
Copenhagen
Tel: +45 38 77 41 18
DSO@kromannreumert.com
1. In your jurisdiction, are there legal requirements for organizations to provide notice of a breach of security for personal data or other company information?

Yes.

Please identify the name of the relevant law(s) or regulation(s).

The regulations can be divided into two areas:

(i) the general regulation, which applies to all entities processing personal data, and

(ii) the specific regulation of breaches of personal data security in the telecommunications sector.

The answers below will be divided in accordance with these two areas.

**General data regulation**: The Danish Act on Processing of Personal Data (Act. no. 429 of 31 May 2000 as amended) (the “DPA”) contains the general regulation of breaches of personal data security and governs all data processing.

**Telecommunications sector**: The Executive Order on Information and Security (Executive Order no. 445 of 11 May 2011) (the “Security Order”), applies to providers of publicly available electronic communications services (“Providers”). Furthermore, breach notices within the telecommunications sector are regulated by the EU-commission’s regulation 611/2013 (the “Resolution”).

2. For each law and regulation identified in Question 1, please describe:

a. **The general scope of the breach notice requirement.**

**General regulation**: All legal entities, including the entities within the telecommunications sector, as well as public authorities may have a notification obligation to the extent it is required by the DPA. This provision is interpreted by the Danish Data Protection Agency which is the regulatory authority in regards to administration of the DPA. This obligation only relates to the affected individuals.

**Telecommunications sector**: Providers are required to give notification in case there is a security breach, which leads to coincidental or unlawful destruction, loss, change of, unlawful passing on of or access to personal data.
Personal data in this respect is understood as any type of personal data that is sent, stored or in any other way processed in relation to the provision of an electronic communication service, cf. section 3 (1) (6) of the Security Order.

b. The definition or standard of a covered “data breach.”

**General regulation:** According to the Danish Data Protection Agency, a data security breach is an action or event that leads to or where there is a risk of an accidental or unlawful destruction, loss, alteration or unauthorized disclosure of personal data transmitted, stored or otherwise processed.

**Telecommunications sector:** As described under the previous question, a data breach is only governed by the Security Order if such breach relates to personal data that is sent, stored or in any other way processed in relation to the provision of an electronic communication service. The definition of personal data is the same as under the PDA.

c. Whether it is mandatory to notify affected individuals.

**General regulation:** Yes. However, not as a general rule. The Danish Data Protection Agency has stated that the provision concerning good practice for the processing of data set out in the Danish Act on Processing of Personal Data DPA, section 5 (1) is applicable for data security breaches. Hence, in a situation of a data security breach, the data controller must consider whether - and if so, how - the affected individuals (the data subjects) should be informed of such breach. In assessing the necessity of such notification, the data controller must take into account the nature of the information and the possible consequences for the individuals. Under any circumstances, the Danish Data Protection Agency recommends that the data controller notify the relevant data subjects in situations where personal data has been leaked to the public against the rules of the Danish Act on Processing of Personal Data.

**Telecommunications sector:** In terms of data security breaches governed by the specific telecommunication regulation, a provider is not required to notify the affected individual/user if the Danish Business Authority finds that the provider has arranged for adequate technical protection measures, and that these technical protection measures have been applied to the data which the security breach relates to. Adequate technical protection measures shall ensure that the data is made non-understandable for all who do not have legal access to the data. To the extent that the notification is required, the data controller must notify the affected individuals as soon as possible which should be construed to be as soon as reasonably possible under the particular circumstances. The following factors may have importance in terms of the appropriate timeframe: the number of the data subjects, the categories of data involved (sensitive vs. non-sensitive data) and the nature of the data security breach.
There are no specific requirements to the content of the notice; however, the content must be relevant for the data subject. Depending on the particular circumstances, the notice should include further information on the security breach (e.g., what exactly has happened), the possible consequences for the data subject in question and the data controller’s actions to limit the consequences (deleting data from the Internet, getting data returned from the wrong receivers, etc.). The wording of the notice must be clear and comprehensible for the data subjects.

If the Provider cannot document to the Danish Business Authorities’ satisfaction that the required technical protection measures are in place, the Provider is obligated to notify the affected individual if the breach can be expected to result in an infringement of the privacy of such individual. Such infringement may, for example, be by way of identity theft, fraud, physical harm, damage to reputation, cf. section 15 (3) of the Security Order.

To the extent that notification of the affected individual is required, the provider must notify the affected individuals without undue delay after the detection of the personal data breach, not to be dependent on the notification of the personal data breach to Danish Business Authority.

The provider must, in its notification to the affected individual, include the content listed in appendix II of the Resolution, more specifically:

1. Name of the Provider
2. Identity and contact details of the data protection officer or other contact point where more information can be obtained
3. Summary of the incident that caused the personal data breach
4. Estimated date of the incident
5. Nature and content of the personal data concerned as referred to in Article 3(2)
6. Likely consequences of the personal data breach for the subscriber or individual concerned as referred to in Article 3(2)
7. Circumstances of the personal data breach as referred to in Article 3(2)
8. Measures taken by the provider to address the personal data breach
9. Measures recommended by the provider to mitigate possible adverse effects
d. Whether it is mandatory to notify any government authorities.
   Yes.

**General regulation:** Neither legal entities or public authorities have any mandatory obligation to notify the Danish Data Protection Agency or any other authority in the event of a data breach. It is highly unusual to approach the authorities in this respect unless the data controller intends to discuss certain issues with the authorities, for example, whether it is required to notify the data subjects.

**Telecommunications sector:** Providers are obligated to notify the Danish Business Authority within 24 hours in the event of a data breach, cf. article 2 of the Resolution. Such notification shall include, if possible, the content set out in appendix I of the Resolution, more specifically:

*Identification of the provider*

1. Name of the provider
2. Identity and contact details of the data protection officer or other contact point where more information can be obtained
3. Whether it concerns a first or second notification: Initial information on the personal data breach (for completion in later notifications, where applicable)
4. Date and time of incident (if known; where necessary an estimate can be made), and of detection of incident
5. Circumstances of the personal data breach (e.g., loss, theft, copying)
6. Nature and content of the personal data concerned
7. Technical and organizational measures applied (or to be applied) by the provider to the affected personal data
8. Relevant use of other providers (where applicable)

*Section 2*

Further information on the personal data breach

1. Summary of the incident that caused the personal data breach (including the physical location of the breach and the storage media involved)
2. Number of subscribers or individuals concerned
3. Potential consequences and potential adverse effects on subscribers or individuals
4. Technical and organizational measures taken by the provider to mitigate potential adverse effects
Possible additional notification to subscribers or individuals

1. Content of notification
2. Means of communication used
3. Number of subscribers or individuals notified

Possible cross-border issues

1. Personal data breach involving subscribers or individuals in other Member States
2. Notification of other competent national authorities. However, if the provider cannot obtain all information necessary to provide the required content listed above, the provider may make an initial notification within 24 hours, which must at least contain the content described under 1-3. The provider shall hereafter make a second notification to the Danish Business Authority as soon as possible after the initial notification, and at the latest within three days following the initial notification. Such second notification shall include, if possible, the remaining content.

e. Whether any other parties may need to be notified of the incident.

No.

f. Whether the above rules are different if the company is acting as a data processor/service provider, and not acting as the data controller/owner of the information at issue.

Yes.
The rules only apply to data controllers.

g. What are the potential penalties for non-compliance with the breach notice obligation?

General regulation: The Danish Data Protection Agency may issue fines for failure to notify in accordance with section 5 (1) on good practice in the DPA. The Danish Data Protection Agency has not issued any fines in relation to this provision and generally, the fines for non-compliance in terms of data protection are rather moderate in Denmark (the largest fine ever issued is DKK 25,000).

Telecommunications sector: Potential penalties for legal entities in the telecommunications sector include fines and criminal liability according to section 23 (1) and (2) in the Security Order. To our knowledge, no fines have ever been issued under the Security Order, and it is not possible to assess the size of any potential fines.
Finland

Hannu Järvinen
Helsinki
Tel: +358 40 550 0306
hannu.jarvinen@borenius.com

Susanna Karlsson
Helsinki
Tel: + 358 20 713 3298
susanna.karlsson@borenius.com
1. In your jurisdiction, are there legal requirements for organizations to provide notice of a breach of security for personal data or other company information?

Yes.

**Please identify the name of the relevant law(s) or regulation(s).**

The Finnish data protection laws do not impose a general obligation to report data security breaches. However, there are certain special regulations in relation to specific industries and entities.

The Information Society Code (917/2014) provides notification requirements for Telecommunications Operators, Added Value Service Providers and Domain Name Registrars.

The Act on Strong Electronic Identification and Electronic Signatures (617/2009) provides notification requirements for Identification Service Providers.

The regulations of the Financial Supervisory Authority (FSA) provide notification requirements for Financial Institutions.

Under the Securities Markets Act (746/2012), listed companies have a general disclosure obligation to disclose information materially affecting the value of a security. We note that a material data breach may give rise to such disclosure obligation.

2. For each law and regulation identified in Question 1, please describe:

a. The general scope of the breach notice requirement.

**Notification requirements under the Information Society Code (917/2014):**

**Telecommunications Operators**

Pursuant to section 275 of the Information Society Code (917/2014), there is an obligation to report data security breaches to the Finnish Communications Regulatory Authority (“FICORA”). Pursuant to section 274 of the Code, there is an obligation to notify subscribers and users of significant information security violations or threats to information security in the services and of anything else that prevents or significantly interferes with communication services.
Added Value Service Providers

Pursuant to section 274 of the Information Society Code, an added value service provider shall notify the users of any significant violation or threat posed to the information security. A “value added service” means a service based on the processing of traffic data or location data for a purpose other than the delivery of a communication.

Domain Name Registrars

Pursuant to section 170 of the Information Society Code, a domain name registrar shall notify FICORA without undue delay of significant violations of information security in its domain name services and of anything that essentially prevents or disturbs such services. A domain name registrar shall also make a notification of the estimated duration and consequences of the disturbance or threats of such disturbances, and of measures undertaken to rectify the situation and to prevent the reoccurrence of such violations.

Notification requirements under the Act on Strong Electronic Identification and Electronic Signatures (617/2009):

Identification Service Providers

Identification Service Providers are required under section 16 of the Act on Strong Electronic Identification and Electronic Signatures (617/2009) to report severe risks and threats to their data security to FICORA and to the Finnish Data Protection Ombudsman when the risk or threat concerns personal data.

Notification requirements under the FSA Regulations:

Financial Institutions

Financial Institutions are, under the Finnish Financial Supervisory Authority (FSA) regulations, obliged to report to the FSA disruptions and faults in services provided to customers, and in payment and IT systems.

The FSA Regulations and Guidelines 8/2014 (Management of operational risk in supervised entities of the financial sector) set conditions for reporting of operational disruptions and faults of the aforementioned entities. The reporting obligation is applicable to (i) credit institutions, (ii) Finnish branches of third country credit institutions, (iii) investment firms governed by chapters 9, 10 and 11 of the Credit Institutions Act in accordance with chapter 6, section 2 of the Investment Services Act, (iv) fund management companies engaged in activities referred to in section 5(2) of the Mutual Funds Act, (v) alternative investment fund managers (AIF managers) providing investment services, (vi) holding companies of credit institutions and investment firms as well as holding companies of conglomerates as referred to in the Act on the Supervision of Financial and Insurance Conglomerates, (vii) central bodies of amalgamations of deposit banks and (viii) payment institutions.
Supervised entities shall immediately inform the FSA of any substantial faults or disruptions in services provided to customers, and in payment and IT systems. Substantial disruptions in money transmission and card payments may be, for example, disruptions and delays affecting a large number of customers or disruptions where customer information has come into the possession of external parties. Disruptions and faults damaging or jeopardising the supervised entity’s capacity to continue its business activities or fulfil its obligations shall also be reported to the FSA without delay. Soon after the first report, the supervised entity shall submit a supplementary report to the FSA with more detailed information on the disruption.

A report shall be submitted for the following disruption types: IT system intrusions, spreading of malicious software to IT systems and denial-of-service attacks. The following disruptions shall also be reported, if they affect the quality of the services provided to the customers: software failures, disruptions in telecommunications, computer downtime and hardware failures as well as delays in money transmission. Beginning 28 February 2016, supervised entities shall submit an annual report to the FSA on losses from operational risks detected in the previous year. The first report shall be submitted on damages detected in 2015. The annual report shall be prepared on the five largest loss events in Euro amounts stemming from operational risks during the course of the calendar year. However, no report need be prepared on damages of less than EUR 10,000.

**General disclosure obligation under the Securities Markets Act (746/2012):**

**Listed companies**

Pursuant to chapter 6, section 4 of the Securities Market Act, Finnish listed companies have a general obligation to disclose information materially affecting the value of a security. As data breaches might materially affect the value of the company’s securities, this information shall in certain cases be published.

**b. The definition or standard of a covered “data breach.”**

There is no specific definition for “data breach”.

Pursuant to the Information Society Code, “information security” means the administrative and technical measures taken to ensure that data is only accessible by those who are entitled to use it, that data can only be modified by those who are entitled to do so, and that data and information systems can be used by those who are entitled to use them. A telecommunications operator shall notify FICORA of any significant information security violations or threats to information security in the services and of anything else that prevents or significantly interferes with communication services. This can mean, for example, a security breach to the operator’s data systems, malware
activation in the operator’s data systems, detected electronic surveillance devices, security breach attempts, abnormal net traffic, hostile login attempts, and detected and unpublished deficiencies in data protection.

c. **Whether it is mandatory to notify affected individuals.**

   Yes.

   **Telecommunications Operators**

   Pursuant to section 274 of the Information Society Code, there is an obligation to notify subscribers and users of significant information security violations or threats to information security in the services and of anything else that prevents or significantly interferes with communication services.

   **Added Value Service Providers**

   Pursuant to section 274 of the Finnish Information Society Code, an added value service provider shall notify the users of any significant violation or threat posed to the information security.

d. **Whether it is mandatory to notify any government authorities.**

   Yes.

   **Telecommunications Operators**

   Pursuant to section 275 of the Finnish Information Society Code (917/2014), there is an obligation to report data security breaches to FICORA.

   **Identification Service Providers**

   Identification Service Providers are required under section 16 of the Act on Strong Electronic Identification and Electronic Signatures (617/2009) to report severe risks and threats to their data security to FICORA and to the Finnish Data Protection Ombudsman when the risk or threat concerns personal data.

e. **Whether any other parties may need to be notified of the incident.**

   Yes.

   **Financial Institutions**

   Financial Institutions are, under the FSA Regulations, obliged to report disruptions and faults in services provided to customers to the FSA, and in payment and IT systems.

   **Listed companies**

   Finnish listed companies have a general disclosure obligation in Finland. As cyber breaches might materially affect the value of the company’s securities, this information shall in certain cases be published.
f. Whether the above rules are different if the company is acting as a data processor/service provider, and not acting as the data controller/owner of the information at issue.

No.

g. What are the potential penalties for non-compliance with the breach notice obligation?

Anyone who deliberately neglects its notification obligation under section 275 of the Information Society Code shall be imposed a fine for a data protection violation in electronic communications. A penalty shall not be ordered if the offence is minor.

The FSA Regulations (e.g., reporting obligation) may be enforced by a conditional fine, unless the failure to comply with the FSA regulation is only minor. The following are generally taken into account when setting the amount of the conditional fine: the nature and scope of the claim, solvency of the company as well as other aspects of the case.

A penalty payment may be imposed if a listed company does not comply with the general disclosure obligation under the Securities Market Act. The amount of the penalty payment is based on an overall assessment where at least the following are taken into account: the nature, gravity and length of the breach, and the solvency of the company.

There is no specific legislation on allocating risk and responsibility for data breaches; however, compensation for damages may become applicable for loss, damage or corruption of data under the Finnish Damages Act (412/1974) or for a breach of contract.
France

Denise Lebeau-Marianna
Paris
Tel: +33 1 44 17 53 33
denise.lebeau-marianna@bakermckenzie.com

Magalie Dansac
Paris
Tel: +33 1 44 17 59 82
Magalie.dansac@bakermckenzie.com
1. In your jurisdiction, are there legal requirements for organizations to provide notice of a breach of security for personal data or other company information?

Yes.

Please identify the name of the relevant law(s) or regulation(s).

Article 34 bis of the French Data Protection Law of 6 January 1978 as revised (FDPL)


2. For each law and regulation identified in Question 1, please describe:

a. The general scope of the breach notice requirement.

FDPL: The law requires the notification of any violation of personal data, which is defined as a violation of security leading accidentally or in an illicit manner to the destruction, loss, alteration, disclosure, or unauthorized access to personal data processed for the purpose of providing electronic communication services to the public.

The Regulation: provides a description of the measures for notification, the manner of notification, the period for which notification should be sent to the data subjects and when such notification may avoided if the data has been, for instance, encrypted and such security measures have been duly checked by the data protection authority.

b. The definition or standard of a covered “data breach.”

See 2(a) above. Notification to the data subjects may be required by the Data Protection Authority only if the breach is likely to affect the data subjects privacy or personal data depending on the nature of data affected (sensitive data or banking data, electronic email, etc.). Exception applies only if the data has been encrypted.

c. Whether it is mandatory to notify affected individuals.

Yes.

Annex II to the Regulation provides a list of the information which must be provided to the affected individuals.

d. Whether it is mandatory to notify any government authorities.
Yes.

The authority is the CNIL (French Data Protection Authority).

The notification must be done online on the CNIL web site.

Notification must be done within 24 hours from the discovery of the violation for the first notification, and 72 hours for the notification supplementing the first one. Notification beyond the prescribed periods is allowed only if such delay is duly justified.

e. Whether any other parties may need to be notified of the incident.

No.

f. Whether the above rules are different if the company is acting as a data processor/service provider, and not acting as the data controller/owner of the information at issue.

No.

g. What are the potential penalties for non-compliance with the breach notice obligation?

Failure to notify a violation of personal data is punishable by imprisonment of five years and a fine of EUR 300,000 (EUR 1,500,000 for a company)(Article 226-17-1 of the Penal Code).
Germany

Wolfgang Fritzemeyer
Munich
Tel: +49 89 55238 154
wolfgang.fritzemeyer@bakermckenzie.com

Michael Schmidl
Munich
Tel: +49 89 55238 211
michael.schmidl@bakermckenzie.com

Matthias Scholz
Frankfurt
Tel: +49 69 29908 203
matthias.scholz@bakermckenzie.com

Holger Lutz
Frankfurt
Tel: +49 69 29908 638
holger.lutz@bakermckenzie.com

Julia Wendler
Munich
Tel: +49 89 55238 261
julia.wendler@bakermckenzie.com
1. In your jurisdiction, are there legal requirements for organizations to provide notice of a breach of security for personal data or other company information?

Yes, German law contains several data breach notification obligations. The following lists the most relevant rules:

(i) Section 42a of the Federal Data Protection Act
(ii) Section 109a of the Telecommunications Act
(iii) Section 15a of the Telemedia Act
(iv) Section 8b of the Act on the Federal Office for Information Security

2. For each law and regulation identified in Question 1, please describe:

a. The general scope of the breach notice requirement.

**Section 42a of the Federal Data Protection Act (FDPA):**

The breach notice requirements apply to:

(i) private and public bodies,
(ii) particular types of stored personal data

(a) sensitive data (racial or ethnic origin, political opinions, religious or philosophical convictions, union membership, health or sex life),
(b) personal data, which are subject to professional secrecy,
(c) personal data related to criminal offences or administrative offences or the suspicion of punishable actions or administrative offences, or
(d) personal data concerning bank or credit card accounts.

**Section 109a of the Telecommunications Act (TCA):**

The breach notice requirements apply to:

(i) anyone who provides publicly available telecommunications services,
(ii) any personal data.

**Section 15a of the Telemedia Act (TMA):**

The breach notice requirements apply to:

(i) service provider according to the TMA,
(ii) customer data and usage data.
For the legal consequences, Section 15a TMA refers to Section 42a FDPA.

**Section 8b of the Act on the Federal Office for Information Security (BSIG):**

The breach notice requirements apply to:

(i) operators of critical infrastructures,

(ii) availability, integrity, authenticity and confidentiality of IT systems, components and processes.

b. The definition or standard of a covered “data breach.”

**Section 42a of the Federal Data Protection Act (FDPA):**

A data breach occurs when:

(i) a responsible person or body recognizes that the respective personal data was unlawfully transferred or otherwise unlawfully revealed to third parties, and

(ii) this causes a threat of serious harm to the data subject’s rights or legitimate interests.

**Section 109a of the Telecommunications Act (TCA):**

A data breach occurs when the protection of personal data is violated, i.e., there is a violation of data security, which leads to the loss, unlawful deletion, modification, storage, dissemination or other illegitimate use of personal data, which are transmitted, stored or otherwise processed in connection with the provision of publicly available telecommunications services, as well as the unlawful access to these.

**Section 15a of the Telemedia Act (TMA):**

A data breach occurs when:

(i) a responsible person or body recognizes that the respective data was unlawfully transferred or otherwise unlawfully revealed to third parties, and

(ii) this causes a threat of serious harm to the data subject’s rights or legitimate interests.

**Section 8b of the Act on the Federal Office for Information Security (BSIG):**

A “data” breach occurs when:

(i) the operator of a critical infrastructure recognizes significant interferences of availability, integrity, authenticity and confidentiality of IT systems, components and processes
(ii) this may cause or has caused a disruption or other adverse effect on the operability of the critical infrastructure.

**c. Whether it is mandatory to notify affected individuals.**

*Section 42a of the Federal Data Protection Act (FDPA):*

Yes.

*Timing*

Individuals have to be informed:

(i) as soon as adequate measures to safeguard the personal data were taken or when such adequate measures were not taken immediately, and

(ii) when such notification would no longer put criminal prosecution at risk.

*Content of the notification*

The notification of individuals must:

(i) describe the nature of the unlawful access, and include

(ii) recommendations for measures to minimize possible harm.

*Section 109a of the Telecommunications Act (TCA):*

Yes.

*Timing*

Individuals (subscribers or other persons) have to be informed immediately, i.e., without undue delay, only in cases where it is reasonable to expect that the infringement violates the rights or protectable interests of such individuals severely.

*Content of the notification*

The notification of individuals must contain:

(i) the nature of the violation of the protection of personal data,

(ii) information on the contact points where further information can be obtained, and

(iii) recommendations for measures to limit the potential adverse effects of the violation of the protection of personal data.

Annex 2 of the EU regulation 611/2013 specifies the content as follows:

(i) Name of the provider

(ii) Identity and contact details of the data protection officer or other contact point where more information can be obtained
(iii) Summary of the incident that caused the personal data breach
(iv) Estimated date of the incident
(v) Nature and content of the personal data concerned
(vi) Likely consequences of the personal data breach for the individual concerned
(vii) Circumstances of the personal data breach
(viii) Measures taken by the provider to address the personal data breach
(ix) Measures recommended by the provider to mitigate possible adverse effects

Exceptions

(i) Notification is not required, when it was proven in the safety concept that the affected personal data is secured by adequate technical measures, in particular using an encryption method which has been recognized as secure; however, even in this case, the competent authority can take the potential adverse effect of the data breach into account and instruct the telecommunication service provider to inform the individuals.

(ii) According to Art 3 (5) EU regulation 611/2013, in exceptional circumstances, where the notification to the individuals may put at risk the proper investigation of the personal data breach, the telecommunication service provider shall be permitted, after having obtained the approval of the competent authority, to delay the notification to the individual until such time as the competent authority deems it possible to notify the individual.

Section 15a of the Telemedia Act (TMA):
Section 15 TMA refers to Section 42a FDPA.

Section 8b of the Act on the Federal Office for Information Security (BSIG):
No.

d. Whether it is mandatory to notify any government authorities.
Yes.

Section 42a of the Federal Data Protection Act (FDPA):
Authority/ Authorities
The competent local data protection authority has to be informed.
Timing
The authority has to be informed immediately, i.e., without undue delay.

Content of the notification
The notification of the authority must:
(i) describe the nature of the unlawful access,
(ii) include recommendations for measures to minimize possible harm, and
(iii) describe the possible harmful consequences of the unlawful access and identify the measures taken.

Section 109a of the Telecommunications Act (TCA):

Authority/ Authorities
Both the BNetzA and the Federal Commissioner for Data Protection and Freedom of Information have to be informed.

Timing
The authorities have to be informed immediately, i.e., without undue delay. According to Art. 2 (2) EU regulation 611/2013 the authorities have to be informed within 24 hours after detection of the violation.

Content of the notification
The notification of the authorities must contain:
(i) the nature of the violation of the protection of personal data,
(ii) information on the contact points where further information can be obtained,
(iii) recommendations for measures to limit the potential adverse effects of the breach of the protection of personal data,
(iv) a description of the consequences of the violation, and
(v) the measures intended to be taken or actually taken.

Annex 1 of the EU regulation 611/2013 specifies the content as follows:
(i) Identification of the provider
   - Name of the provider
   - Identity and contact details of the data protection officer or other contact point where more information can be obtained
   - Whether it concerns a first or second notification
(ii) Initial information on the personal data breach (for completion in later notifications, where applicable)

- Date and time of incident (if known; where necessary an estimate can be made), and of the detection of the incident
- Circumstances of the personal data breach (e.g., loss, theft, copying)
- Nature and content of the personal data concerned
- Technical and organizational measures applied (or to be applied) by the provider to the affected personal data
- Relevant use of other providers (where applicable)

(iii) Further information on the personal data breach

- Summary of the incident that caused the personal data breach (including the physical location of the breach and the storage media involved):
  - Number of subscribers or individuals concerned
  - Potential consequences and potential adverse effects on subscribers or individuals
  - Technical and organizational measures taken by the provider to mitigate potential adverse effects

(iv) Possible additional notification to subscribers or individuals

- Content of notification
- Means of communication used
- Number of subscribers or individuals notified

(v) Possible cross-border issues

- Personal data breach involving subscribers or individuals in other Member States
- Notification of other competent national authorities

Section 15a of the Telemedia Act (TMA):

Section 15 TMA refers to Section 42a FDPA.

Section 8b of the Act on the Federal Office for Information Security (BSIG):

Authority

The Federal Office for Information Security has to be informed.
Timing
The authority must be informed immediately, i.e., without undue delay.

Content of the notification
The notification must contain details of the interference and the technical circumstances surrounding the presumed or actual cause, the affected IT systems, the type of affected components and processes, and details of the industry sector of the operator. The identification of the operator is only necessary if the interference in fact caused the disruption or other adverse effect on the operability of the critical infrastructure.

e. Whether any other parties may need to be notified of the incident.

Section 42a of the Federal Data Protection Act (FDPA):
Where notifying the individuals would require unreasonable effort, in particular due to the large number of cases involved, such notification may be replaced by public advertisements of at least one-half page in size and in at least two national daily newspapers, or by other equally effective measures for notifying the data subjects.

Section 109a of the Telecommunications Act (TCA):
According to Art 3 (7) EU regulation 611/2013, where the telecommunication service provider having a direct contractual relationship with the end user, despite having made reasonable efforts, is unable to identify all individuals who are likely to be adversely affected within the timeframe in which the individuals must be notified, the telecommunication service provider may notify those individuals through advertisements in major national or regional media. The telecommunication service provider shall continue to make all reasonable efforts to identify those individuals and to notify them as soon as possible.

Section 15a of the Telemedia Act (TMA):
Section 15 TMA refers to Section 42a FDPA:

Section 8a Act on the Federal Office for Information Security (BSIG):
No.
f. Whether the above rules are different if the company is acting as a data processor/service provider, and not acting as the data controller/owner of the information at issue.

Section 42a of the Federal Data Protection Act (FDPA):

The data controller/owner is subject to the notification obligations. However, the data processor/service provider is under a statutory and typically also a contractual obligation to inform the data controller/owner immediately in case he becomes aware of a security breach so that the data controller/owner can fulfill its notification requirements.

Section 109a of the Telecommunications Act (TCA):

The telecommunication services provider is subject to the notification obligation. However, the data processor/service provider is under a statutory and typically also a contractual obligation to inform the telecommunication service provider immediately in case he becomes aware of a security breach so that the telecommunication services provider can fulfill its notification requirements.

Section 15a of the Telemedia Act (TMA):

The telemedia provider is subject to the notification obligation. However, the data processor/service provider is under a statutory and typically also a contractual obligation to inform the telemedia provider immediately in case he becomes aware of a security breach so that the telemedia provider can fulfill its notification requirements.

Section 8a of the Act on the Federal Office for Information Security (BSIG):

This rules applies to operators of critical infrastructure. It is not linked to personal data.

g. What are the potential penalties for non-compliance with the breach notice obligation?

Section 42a of the Federal Data Protection Act (FDPA):

Up to EUR 300,000 and a higher amount to skim any profits derived from the breach.

In case non-compliance was committed willfully in exchange for payment or with the intention to enrich oneself or another person or of harming another person, the penalty can be imprisonment of up to two years or a criminal fine.
Section 109a of the Telecommunications Act (TCA):
Up to EUR 100,000 or more per incident.

Section 15a of the Telemedia Act (TMA):
Section 15 TMA refers to Section 42a FDPA.

Section 8a of the Act on the Federal Office for Information Security (BSIG):
Up to EUR 50,000 per incident.
Greece

Vassilis Constantes
Athens
Tel: +30 210 720 6900
v.constantes@vplaw.gr
1. In your jurisdiction, are there legal requirements for organizations to provide notice of a breach of security for personal data or other company information?

Yes.

Please identify the name of the relevant law(s) or regulation(s).

(1) Law 2472/1997 on the protection of individuals with regard to the processing of personal data ("PIPPD")

(2) Law 3471/2006 on the protection of personal data and privacy in the electronic communications sector

2. For each law and regulation identified in Question 1, please describe:

a. The general scope of the breach notice requirement.


b. The definition or standard of a covered “data breach.”

(1) PIPPD does not provide a specific definition of “data breach.” However, in principle, the data controller must implement appropriate organizational and technical measures to secure data and protect them against accidental or unlawful destruction, accidental loss, alteration, unauthorized disclosure or access as well as any other form of unlawful processing.

(2) According to the definition provided in Law 3471/2006, “personal data breach” means security breach that leads to accidental or unlawful destruction, loss, distortion, unauthorized dissemination or unauthorized access to personal data that was transferred, stored or was subject to processing in any other manner in connection with the provision of a publicly available electronic communications services.

c. Whether it is mandatory to notify affected individuals.

Yes.

(1) PIPPD does not set any specific requirements for the timing or the content of notification of the data subject.

(2) (i) In para. 6 of article 12 of Law 3471/2006 it is stated that “when the personal data breach may have unpropitious consequences to the personal data or the private life of the subscriber or other person, the
provider must notify without undue delay the affected subscriber or the
affected person. The notification of the previous section includes at least
a description of the nature of the personal data breach and the contact
points from which further information can be obtained as well as
recommendations that can limit potential unfavorable results from the
personal data breach.”

(ii) in para. 7 of the same article, it is stated that “the notification of the
affected subscriber or affected person of the personal data breach is not
necessary, if the provider has proved to the competent authorities in a
satisfactory manner that he/she has applied appropriate technical security
measures and that these measures were applied to the data subject to
the security breach. These measures for technological protection must at
least include secure data encryption so that unauthorized access is not
possible. If the provider has not provided notification according to para. 6
of the present article, the competent authorities, after examining the
possible unpropitious consequences from the breach, can ask him/her to
do so.”

d. **Whether it is mandatory to notify any government authorities.**
   Yes.

   (1) PIPPD does not provide for a mandatory obligation to notify any authority
   in an event of data breach.

   (2) In para. 5 of article 12 of Law 3471/2006, it is stated that “In case of a
   personal data breach, the provider of publicly available electronic
   communications services should notify the Hellenic Authority for Ensuring
   the Secrecy of Communications and the Hellenic Personal Data
   Protection Authority of the breach without undue delay. The notification to
   the competent authorities includes at least a description of the nature of
   the personal data breach and the contact points from which further
   information can be obtained. Moreover, it should describe the
   consequences of the breach and the measures that were suggested or
   taken by the provider to deal with the breach.”

e. **Whether any other parties may need to be notified of the
   incident.**
   No.

f. **Whether the above rules are different if the company is acting
   as a data processor/service provider, and not acting as the
   data controller/owner of the information at issue.**
   No.
g. What are the potential penalties for non-compliance with the breach notice obligation?

None of the above laws expressly provide for potential penalties for non-compliance with the breach notice obligation.
Hong Kong

Susan Kendall
Hong Kong
Tel: +852 2846 2411
susan.kendall@bakermckenzie.com

Paolo Sbuttoni
Hong Kong
Tel: +
paolo.sbuttoni@bakermckenzie.com
1. In your jurisdiction, are there legal requirements for organizations to provide notice of a breach of security for personal data or other company information?

Yes.

**Please identify the name of the relevant law(s) or regulation(s).**

The Office of the Privacy Commissioner for Personal Data ("PCPD") published a Guidance Note on the Data Breach Handling and the Giving of Data Breach Notifications ("Breach Guidance Note").

2. For each law and regulation identified in Question 1, please describe:

a. **The general scope of the breach notice requirement.**

The Breach Guidance Note confirms that it is not a statutory requirement on data users to inform the PCPD or any parties about a data breach incident. However, data users are encouraged to adopt a system of notification for proper handling of data breach incidents. PCPD recommends data users to seriously consider notifying the data subjects and the relevant parties where data subjects can be identified and the risk of harm is reasonably foreseeable. Depending on the circumstances of each case, the Breach Guidance Note also provides guidance on:

(i) who the notification should be given to,

(ii) what should be included in the notification,

(iii) when to issue the notification, and

(iv) how to notify the data breach.

In order to submit a data breach notification to the PCPD, data users can fill out the Data Breach Notification Form and submit it through the Internet.

b. **The definition or standard of a covered “data breach.”**

According to the Breach Guidance Note, a data breach is generally taken to be a suspected breach of data security of personal data held by a data user, which exposes these data to the risk of loss, unauthorized or accidental access, processing, erasure or use. Examples of data breaches include the loss of personal data kept in storage, improper handling or disposal of personal data, a database containing personal data being hacked or accessed by unauthorized third parties, and the leakage of data caused by file-sharing software in a computer.
c. Whether it is mandatory to notify affected individuals.
   No.

d. Whether it is mandatory to notify any government authorities.
   No.

e. Whether any other parties may need to be notified of the incident.
   No.

f. Whether the above rules are different if the company is acting as a data processor/service provider, and not acting as the data controller/owner of the information at issue.
   Yes.

   The obligations in the Personal Data (Privacy) Ordinance ("PDPO") only apply to data users and, therefore, processors are beyond the scope of the requirements. However, if a data user becomes aware of a data processor breach incident, the data user is responsible for complying with the PDPO and acting in accordance with the Breach Guidance Note in respect of the breach.

g. What are the potential penalties for non-compliance with the breach notice obligation?
   Since data breach notification is not mandatory, there is no penalty for non-compliance. However, in order to mitigate the loss and damage caused to the affected data subjects, PCPD considers it prudent and advisable for data users to consider giving a data breach notification.
Hungary

Ines K. Radmilovic
Budapest
Tel: +36 1 302 3330
ines.radmilovic@bakermckenzie.com

Adam Liber
Budapest
Tel: +36 1 302 3330
Adam.Liber@bakermckenzie.com

Orsolya Gondos
Budapest
Tel: +36 1 302 3330
orsolya.gondos@bakermckenzie.com
1. In your jurisdiction, are there legal requirements for organizations to provide notice of a breach of security for personal data or other company information?

Yes, but only for telecoms operators.

Please identify the name of the relevant law(s) or regulation(s).

Law.

Act C of 2003 on Electronic Communications (the “Ehk.”)

2. For each law and regulation identified in Question 1, please describe:

a. The general scope of the breach notice requirement.

In Hungary, data breach notification obligations apply if the personal data of telecom services subscribers is breached. The notification must be provided to the National Media and Infocommunications Authority (“NMHH”).

b. The definition or standard of a covered “data breach.”

The Ehk. defines a data breach as a breach of security leading to the accidental or unlawful use or processing of personal data, meaning, in particular, the destruction, loss, alteration, unauthorized disclosure of, or access to personal data transmitted, stored or otherwise processed in connection with the provision of a publicly available electronic communications service. No exceptions apply to the breach notification obligation of service providers; any breach event must be promptly reported to the NMHH.

c. Whether it is mandatory to notify affected individuals.

Affected individuals must be notified only if the personal data breach is likely to adversely affect the personal data or privacy of a subscriber or of other private individuals. In such cases, the provider of electronic communications services must also notify the subscriber or private individual of the breach without undue delay, but within 24 hours at the latest. However, notification to a subscriber or private individual concerned is not required if the telecoms services provider has demonstrated to the satisfaction of the NMHH that it has implemented appropriate technological protection measures and that those measures were applied to the data affected by the security breach. Such technological protection measures must be capable of rendering the data unintelligible to any person who is not authorized to access it.

If the service provider has not notified the subscriber or private individual of the personal data breach, the NMHH, having evaluated the likely adverse effects of the breach, following consultation with the National Authority for
Data Protection and Freedom of Information ("NAIH"), may require the service provider to do so.

If given, the data breach notification to the affected individuals must include the following information:

i. the name of the service provider;

ii. the name and contact information of the service provider’s internal data protection officer or any other contact person providing information;

iii. a summary of the data breach;

iv. the estimated date and time of the breach;

v. the nature and content of the personal data affected;

vi. the potential consequences and adverse effects to the subscribers, users or other private individuals;

vii. the circumstances of the breach;

viii. the measures taken to manage the breach;

ix. the measures proposed to mitigate the potential adverse effects of the breach; and

x. whether the NMHH has been notified of the breach.

d. **Whether it is mandatory to notify any government authorities.**

Yes. If a personal data breach occurs, the telecoms services provider must without undue delay, but within 24 hours at the latest, notify the NMHH concerning that breach. If the telecom services provider does not possess some of the data required to be included in that notification, the service provider must commence an internal investigation, and, within 24 hours of the breach, notify the NMHH of the following information (the “first notification”):

i. the name of the service provider;

ii. the name and contact information of the service provider’s internal data protection officer;

iii. whether the notification is the first or second notification;

iv. the date and time of the breach (estimates, if necessary) and of the detection of the breach;

v. the method and circumstances of the breach;

vi. the nature and content of the personal data affected;
vii. the technical and organizational measures applied or proposed to be applied for the protection of personal data; and

viii. any connections related to the use of another service provider.

After the first notification, the telecoms service provider must gather the information necessary for the second notification, which must be submitted without undue delay, but within 72 hours from the first notification (the “second notification”). The second notification must include the following information:

i. a summary of the event, indicating the material place of breach and the data storage media affected as well;

ii. the number of affected subscribers, users or other private individuals;

iii. a description of the potential consequences and adverse effects to the subscribers, users or other private individuals; and

iv. the technical and organizational measures applied to mitigate the potential adverse effects.

If the telecoms service provider can gather all of the above information within 24 hours from the detection of the breach, then said information must be included in the first notification, which then will be the single notification to NMHH concerning the breach.

If the telecoms service provider is unable to collect all of the above information within 72 hours from the first notification, the service provider must, within that 72-hour deadline, provide all information available regarding the breach and must provide a detailed report of the reasons why the service provider will be able to present all of the required information only after said deadline.

If the affected data subjects were notified before the NMHH was notified, the notification to the NMHH must include the following information:

i. the date and content of the notification to the data subjects, including contact points at which the subscribers, users or other private individuals can obtain additional information regarding the breach;

ii. the communication means used for that notification; and

iii. the number of notified subscribers, users or private individuals.

If the breach has international aspects or effects, the notification to NMHH must include the following information (if it is available):

i. whether the breach has affected any subscriber, user or other private individual residing in a different EU member state; and

ii. information regarding the telecom services provider’s notification to other national authorities concerning the data breach.
Additionally, telecoms service providers must maintain an inventory of personal data breaches, comprising: the material facts surrounding each breach; its effects; and the remedial action taken by the provider. The inventory must include all facts and circumstances and information that are considered sufficient to enable the NMHH to verify compliance by the telecoms service provider of the obligation to notify the affected individuals.

Until the closure of its investigation, the telecoms service provider must inform the NMHH monthly about the information arising from its investigation in the past month.

e. Whether any other parties may need to be notified of the incident.

No notification to other parties is required.

f. Whether the above rules are different if the company is acting as a data processor/service provider, and not acting as the data controller/owner of the information at issue.

No.

g. What are the potential penalties for non-compliance with the breach notice obligation?

The NMHH may impose the following sanctions in case of non-compliance with the electronic communications regulations, including, for example, the failure to comply with data breach notification requirements:

i. a fine of 0.1 per cent of the infringer’s turnover (in the absence of any information as to turnover, or if the net turnover had not been disclosed, the fine may be between HUF 50,000 and 100 million, in the NMHH’s discretion);

ii. in case of repeat offenders, a fine on the executive officer of the infringing entity, in an amount between HUF 50,000 and 3 million, in the NMHH’s discretion;

iii. in the event of a serious and repeated breach of the obligation, the suspension of the telecoms service provider’s authorization for a period ranging from 10 to 90 days, in the NMHH’s discretion;

iv. in the event of a particularly serious and repeated offense, prohibiting the telecoms service provider from pursuing electronic communications activities.

The NMHH must impose the sanctions, depending on the nature of the infringement, taking into account: the gravity of the infringement; whether it was committed on one or several occasions, or on an ad hoc or continuous basis; its duration; the pecuniary benefits derived from the infringement; the
harm caused by the infringement; the number of persons aggrieved or jeopardized; the damage caused by the infringement and the impact of the infringement on the market; and such other considerations needed to be taken into account in the particular case.

If, however, the infringement is considered insignificant and no re-occurrence is established, the NMHH may issue a warning to the telecoms service provider concerning the occurrence of the infringement, and, without imposing any further legal sanctions, may order the infringer to discontinue the unlawful conduct within a deadline established by NMHH or to refrain from any future infringement and to act as required by law (for which purpose the NMHH may set particular conditions).
Iceland

Hjördis Halldórsdóttir
Reykjavík
Tel: + 354 5 400 300
hjordis@logos.is
1. In your jurisdiction, are there legal requirements for organizations to provide notice of a breach of security for personal data or other company information?

Yes.

Please identify the name of the relevant law(s) or regulation(s).


2. For each law and regulation identified in Question 1, please describe:

a. The general scope of the breach notice requirement.

There is no mandatory requirement based on Icelandic data protection legislation (Act No 77/2000 on The Protection of Privacy as regards the Processing of Personal Data), to report data security breaches or losses to the Icelandic Data Protection Authority or data subjects. However, a notice is considered as good practice, particularly if the security breach is major.

Providers of electronic communications undertakings, however, are required to notify their customers of a security breach, based on Article 47 of the Electronic Communications Act No 81/2003.

Based on Rules No 1221/2007, which have been implemented on the basis of The Electronic Communications Act, customers must be notified of any security incidents that cause disturbance to continuous electronic communications services, if the security of a specific network is compromised or if customer information is seriously jeopardized due to a security risk on the electronic communications networks.

Providers of electronic communications undertakings must have clear and effective procedures for such notifications. The relevant service criteria must appear on a website or in a comparable medium; for example, in customer agreements. The notification must state, at a minimum, what effect the incident has or may have, the measures that the provider of the electronic communications undertaking will take, and advice to customers if such an incident occurs.

If the measures that providers of electronic communications undertakings adopt in their electronic communications networks do not apply to a specific security incident, the provider must advise their customers of the measures to counteract vulnerabilities to prevent the spread of the security incident into their systems; for example, to recommend a special software or cryptographic technology for use in public IP networks, including the Internet.
b. The definition or standard of a covered “data breach.”
There is no duty to provide notice of a breach of security based on Icelandic data protection legislation. In relation to the notification duty on electronic communications undertakings, a notification is only necessary if security of a specific network is compromised or if customer information is seriously jeopardized due to a security risk on the electronic communications networks.

c. Whether it is mandatory to notify affected individuals.
Yes.
In relation to the notification duty on electronic communications undertakings, the notification must state, at a minimum, what effect the incident has or may have, the measures that the providers of electronic communications undertaking will take, and advice to customers if such an incident occurs. There is however no standard for the timing.

d. Whether it is mandatory to notify any government authorities.
No.

e. Whether any other parties may need to be notified of the incident.
No.

f. Whether the above rules are different if the company is acting as a data processor/service provider, and not acting as the data controller/owner of the information at issue.
No.

g. What are the potential penalties for non-compliance with the breach notice obligation?
Infringement of the Electronic Communications Act may result in fines or imprisonment of up to two years, in case of serious or repeated violations, based on Article 74 of the Act.
India

Probir Roy Chowdhury
Bangalore
Tel: +91-80-43503618
probir@jsalaw.com

Sajai Singh
Bangalore
Tel: +91-98450 78666
sajai@jsalaw.com
1. In your jurisdiction, are there legal requirements for organizations to provide notice of a breach of security for personal data or other company information?

Yes.

**Please identify the name of the relevant law(s) or regulation(s).**

The Information Technology (The Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules, 2013 (“CERT-In Rules”) issued by the Government of India under the Information Technology Act, 2000 (“IT Act”).

2. For each law and regulation identified in Question 1, please describe:

   a. **The general scope of the breach notice requirement.**

   The breach notice requirement prescribed under the CERT-In Rules applies uniformly to all kinds of data and across all industry sectors. Any event that violates an applicable security policy and results in the unauthorized access and use of IT systems and data is reportable under the CERT-In Rules.

   b. **The definition or standard of a covered “data breach.”**

   The CERT-In Rules use the term Cyber Security Incident to mean any real or suspected adverse event in relation to cyber security that violates an explicitly or implicitly applicable security policy resulting in unauthorized access, denial of service or disruption, unauthorized use of a computer resource for processing or storage of information or changes to data or information without authorization.

   c. **Whether it is mandatory to notify affected individuals.**

   No.

   d. **Whether it is mandatory to notify any government authorities.**

   Yes.

   The authority in this regard is the Indian Computer Emergency Response Team (“CERT-In”). A corporate entity which is a victim of a Cyber Security Incident is required to report the incident to CERT-In within a “reasonable time,” and in all cases such report should be made early enough to leave scope for remedial action.

   e. **Whether any other parties may need to be notified of the incident.**

   No.
f. Whether the above rules are different if the company is acting as a data processor/service provider, and not acting as the data controller/owner of the information at issue.

No.

g. What are the potential penalties for non-compliance with the breach notice obligation?

No specific penalty has been prescribed under the CERT-In Rules or the IT Act for non-compliance with the breach notice obligations. Therefore, an entity that fails to notify a Cyber Security Incident to CERT-In would be liable to pay the residuary penalty prescribed under the IT Act for non-compliance, i.e., Rs. 25,000 (Twenty Five Thousand Rupees only, or approximately US $385).
Indonesia

Mark Innis
Jakarta
Tel: +62 21 2960 8618
mark.innis@bakernet.com

Susie Beaumont
Jakarta
Tel: +62 21 2960 8608
susie.beaumont@bakernet.com

Alvira M. Wahjosoedibjo
Jakarta
Tel: +62 21 2960 8503
alvira.m.wahjosoedibjo@bakernet.com
1. In your jurisdiction, are there legal requirements for organizations to provide notice of a breach of security for personal data or other company information?

Yes.

Please identify the name of the relevant law(s) or regulation(s).

Law.

No. 11 of 2008 on Electronic Information and Transaction ("EIT Law") and its implementing regulation, Government Regulation No. 82 of 2012 on the Implementation of Electronic Systems and Transactions ("GR 82").

In addition, please note that the Ministry of Communications and Informatics ("MOCI") is preparing a draft regulation specifically on data protection ("Draft Regulation"). However, the MOCI cannot confirm when the regulation will be issued. Any references to the Draft Regulation made in this document are for information purposes only as the Draft Regulation has not been enacted yet and may be subject to change.

2. For each law and regulation identified in Question 1, please describe:

a. The general scope of the breach notice requirement.

The one specific provision on data breach under current regulations is in Article 15.2 of GR 82, which states that if there is any failure in personal data confidentiality protection, the relevant electronic system operator must notify the owner of the personal data in writing. There is no provision on when the notification should be made; however to be prudent, the notice should be made immediately after the electronic system operator becomes aware of the breach.

In addition, under the Draft Regulation, the written notice must be made in the following manner: (i) must include the reason or cause of the failure in personal data confidentiality protection; (ii) can be made electronically if the data owner has given its consent for it, which is stated at the time of the data collection; and (iii) the electronic system operator must ensure the notice is received by the data owner if the failure has the potential of losses to the relevant data owner.

b. The definition or standard of a covered “data breach.”

There is no specific provision (nor is there any exception) on the definition or standard of a covered “data breach.” Therefore, every breach of personal data can be considered as a failure in personal data confidentiality protection and the notice requirement will apply.
c. **Whether it is mandatory to notify affected individuals.**
Yes.

As mentioned in point 2(a) above, GR 82 requires the electronic system operator to notify the data owner in writing in the event of a data breach. There are no further provisions on the format of the notice or the timing for the notice to be made.

d. **Whether it is mandatory to notify any government authorities.**
No.

However, GR 82 provides that in the event of a system failure or disruption that has serious impact (regardless if there is any data breach) as a result of another party’s action to the electronic system, the electronic system operator must secure the data and promptly report the failure or disruption to the law enforcer.

e. **Whether any other parties may need to be notified of the incident.**
No.

f. **Whether the above rules are different if the company is acting as a data processor/service provider, and not acting as the data controller/owner of the information at issue.**
No.

EIT Law and GR 82 do not differentiate between data controller/owner and data processor/service provider. The term “electronic system operator” means any party who provides, processes and/or operates electronic systems to the electronic system users for its own interest and/or others. Theoretically, if the data processor/service provider also receives personal data to be processed, then in the event of the data breach, the notice requirement will also apply to them.

g. **What are the potential penalties for non-compliance with the breach notice obligation?**
The EIT Law and GR 82 do not provide any specific criminal sanctions in respect of a data breach. However, A violation of GR 82 is subject, where the relevant party is a legal entity, to administrative sanctions in the form of warning letters, administrative fines, suspension of data processing, and deregistration as a business.
Ireland

John Cahir
Dublin
Tel: +353 1 649 2000
jcahir@algoodbody.com

Alison Quinn
Dublin
Tel: +353 1 649 2461
alquinn@algoodbody.com
1. In your jurisdiction, are there legal requirements for organizations to provide notice of a breach of security for personal data or other company information?

Yes.

**Please identify the name of the relevant law(s) or regulation(s).**

The Data Protection Acts 1988 and 2003 (the “DP Acts”) do not contain a mandatory breach notice requirement; however, the Office of the Data Protection Commissioner (“ODPC”) has issued a code of practice (the “Code”) recommending notification to the ODPC where personal data has been put at risk of unauthorized disclosure, loss, destruction or alteration (except where the data can be considered inaccessible and unintelligible due to proper security). While the Code is non-binding in nature, it is considered best practice and compliance is recommended.

Separate obligations apply to “publicly available communications services” providers (such as telecommunications companies and ISPs) under the European Communities (Electronic Communications Networks and Services) (Privacy and Electronic Communications) Regulations 2011 (SI 336 of 2011) (the “Privacy Regulations”). Under the Privacy Regulations there is a requirement to report without undue delay any personal data breach to the ODPC, even where it considers the data would be unintelligible to third parties.

2. For each law and regulation identified in Question 1, please describe:

a. **The general scope of the breach notice requirement.**

   Please see 1 above.

b. **The definition or standard of a covered “data breach.”**

   The DP Acts do not specifically define a “data breach,” however, a data controller is under a specific obligation to take appropriate measures to protect the security of personal data and to prevent “any unauthorized access to, or unauthorized alteration, disclosure, loss or destruction of data and any other unlawful forms of processing, whether in manual or electronic form.”

   The Code states that all incidents in which personal data has been put at risk should be notified by the data controller to the ODPC as soon as the data controller becomes aware, except where (i) the consequences of the incident were reported to the data subjects directly without delay; and (ii) it affects no more than 100 data subjects; and (iii) it does not include sensitive personal data or personal data of a financial nature. A personal data breach under the
Privacy Regulations is defined as a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed in connection with the provision of a publicly available electronic communications service in the European Union. It is not necessary to notify individuals if the ODPC is satisfied that the data would be unintelligible to third parties.

c. **Whether it is mandatory to notify affected individuals.**
No.

d. **Whether it is mandatory to notify any government authorities.**
No, except as required under the Privacy Regulations (see 1 above).

e. **Whether any other parties may need to be notified of the incident.**
Yes.

There is no requirement to notify any other parties; however, the Code states that, in appropriate cases, data controllers should notify organizations that may be in a position to assist in protecting data subjects including where relevant the An Garda Siochana and financial institutions.

f. **Whether the above rules are different if the company is acting as a data processor/service provider, and not acting as the data controller/owner of the information at issue.**
Yes.

A data processor must report breaches of personal data security to the relevant data controller as soon as they become aware of the incident.

g. **What are the potential penalties for non-compliance with the breach notice obligation?**

An organization that is involved in a data breach situation may be subject to an administrative fine, penalty or sanction, or civil actions, class actions, and/or a criminal prosecution. Failure to report a breach as required by the Privacy Regulations is an offence and such undertakings can be subject to criminal prosecution with fines of up to 5,000 and on indictment 250,000 per offence.

The ODPC may investigate the circumstances surrounding the personal data security breach and can use the regular enforcement powers to compel appropriate action to protect the interests of data subjects. Under section 10 of the DP Acts, the ODPC may require a data controller or data processor to take whatever steps the ODPC considers appropriate to comply with the terms of the DP Acts. The ODPC exercises this power by providing a written
notice, called an “enforcement notice,” to the data controller or data processor. It is an offence to fail or refuse to comply with an enforcement notice without reasonable excuse.

The penalty for an offence under the DP Acts is a fine of up to EUR 3,000 on summary conviction or a maximum fine of EUR 100,000 on conviction on indictment.
Israel

Daniel Reisner
Tel Aviv
Tel: +972 3 692 2884
reisnerd@hfn.co.il

Nurit Dagan
Tel Aviv
Tel: +972 3 692 7424
dagan@hfn.co.il
1. In your jurisdiction, are there legal requirements for organizations to provide notice of a breach of security for personal data or other company information?

There are no general requirements for organizations to provide notice of a breach of security for personal data or other company information under the Israeli Protection of Privacy Law, 1981, the regulations enacted thereunder and the guidelines issued by the Israeli DPA – ILITA (Information Law and Technology Authority).

In October 2013, a non-governmental draft bill entitled: Draft Bill Protection of Privacy Law (Amendment- Report on Security Breach in a Database), 2013, was initiated by a few members of Parliament. The purpose of this draft bill is to require the owner or holder of a database to report cases of penetration of their databases to data subjects and to the Registrar of Databases, and in addition, to authorize the Registrar to impose fines in this regard. Currently, the enactment process of this bill is on hold and it is not clear if and when it will be resumed, and what will be its final version.

In addition, notification requirements might exist under certain specific laws and regulations relating to specific sectors (such as the financial sector) and, therefore, this matter should be further reviewed on a case-by-case basis with respect to each sector.

2. For each law and regulation identified in Question 1, please describe:

a. **The general scope of the breach notice requirement.**
   
   No general requirements under the Israeli Protection of Privacy Law, although sector specific laws may apply.

b. **The definition or standard of a covered “data breach.”**
   
   Not applicable.

c. **Whether it is mandatory to notify affected individuals.**
   
   Not applicable.

d. **Whether it is mandatory to notify any government authorities.**
   
   Not applicable.

e. **Whether any other parties may need to be notified of the incident.**
   
   Not applicable.
f. Whether the above rules are different if the company is acting as a data processor/service provider, and not acting as the data controller/owner of the information at issue.

Not applicable.

g. What are the potential penalties for non-compliance with the breach notice obligation?

Not applicable.
Italy

Francesca Gaudino
Milan
Tel: +39 02 76231 452
francesca.gaudino@bakermckenzie.com

Lorenzo de Martinis
Milan
Tel: +39 02 76231 334
Lorenzo.demartinis@bakermckenzie.com
1. In your jurisdiction, are there legal requirements for organizations to provide notice of a breach of security for personal data or other company information?

Yes.

Please identify the name of the relevant law(s) or regulation(s).

Legislative Decree June 30 2003 - n. 196 and the subsequent amendments and integrations - the Data Protection Code, in particular Art. 32-bis.

2. For each law and regulation identified in Question 1, please describe:

a. The general scope of the breach notice requirement.

The breach notice requirement applies only to providers of publicly available electronic communications services.

According to Art. 4 - pr. 3 letter g-bis of the Data Protection Code: “'personal data breach' shall mean a security breach leading, accidentally or not, to the destruction, loss, alteration, unauthorised disclosure of or access to personal data transmitted, stored or otherwise processed in the context of the provision of a publicly available communications service.”

b. The definition or standard of a covered “data breach.”

Notification of personal data breach is not required when the provider of publicly available electronic communications services has provided adequate evidence to the Italian Data Protection Authority that the data covered by the breach were protected with technological measures such that the data has become unintelligible to any entity not authorized to access such data.

c. Whether it is mandatory to notify affected individuals.

Yes.

When a personal data breach occurs, the provider of publicly available electronic communications services shall promptly notify the Italian Data Protection Authority and, when the data breach is likely to have adverse effects on the personal data or on the privacy of either the contracting party or another person, the provider shall also promptly notify said contracting party or person.

In consideration of the possible negative consequences of the personal data breach, the Italian Data Protection Authority may directly order the provider to notify the contracting party or another person who may be adversely affected by the breach, in case of failure by said provider to give prompt notification.
The notification shall include the following information at a minimum: a description of the nature of the personal data breach, indication of contact points available to provide further information, a list of recommended steps to be adopted in order to limit possible negative consequences of the personal data breach, a description of the consequences of the breach as well as of the measures proposed or already taken by the provider in order to cure the breach.

In addition, the provider of publicly available electronic communications services shall keep an updated inventory of the personal data breaches suffered, also including description of the features of the breach, relevant effects as well as description of the measures implemented to cure the breach and other information that may be necessary for the Italian data protection authority to verify compliance with the applicable provisions of the Data Protection Code.

d. **Whether it is mandatory to notify any government authorities.**

Yes.

Please refer to question 2 (c) above.

e. **Whether any other parties may need to be notified of the incident.**

Yes.

Any person who may suffer detrimental effects in terms of personal data and privacy shall be notified of the data breach, according to the above conditions.

While it is not a mandatory legal requirement, notification of a data breach may trigger media attention in the affected region/area and may prompt national consumer reporting agencies to take action.

Please refer to question 2 (c) above.

f. **Whether the above rules are different if the company is acting as a data processor/service provider, and not acting as the data controller/owner of the information at issue.**

Yes.

The Data Protection Code provides that if the provider of a publicly available electronic communications service assigns delivery/performance of the service to third parties, the third party processor must promptly notify the provider of any and all events and information that are necessary for the provider to comply with the applicable requirements on personal data breach set forth by the Data Protection Code.
g. What are the potential penalties for non-compliance with the breach notice obligation?

Art. 162-ter of the Data Protection Code (*Penalties against Providers of Publicly Available Electronic Communications Services*) provides that in case of a failure to notify the data breach to (i) the Italian Data Protection Authority, an administrative fine shall be imposed ranging between EUR 25,000 and 150,000; (ii) the contracting party or any other person involved in the data breach, an administrative fine shall be imposed ranging between EUR 150 and 1,000 per contracting party or individual (the same will apply in case the notification is delayed). In any case, the administrative fine under point (ii) above cannot exceed the threshold of 5% percent of the turnover of the provider in the last accounting year prior to the issuance of the administrative fine. The Italian Data Protection Authority may increase the fines to up to four times in consideration of the economic conditions of the offender.

Failure to keep an updated inventory of data breaches is punishable with a fine ranging from EUR 20,000 to 120,000.

Lastly, the same sanctions apply to third parties to which the provider of publicly available electronic communications services has entrusted the delivery/performance of the services if said third parties fail to provide the provider with the information as per Section 32-*bis* of the Italian Data Protection Code.
1. In your jurisdiction, are there legal requirements for organizations to provide notice of a breach of security for personal data or other company information?

Yes.

Please identify the name of the relevant law(s) or regulation(s).

The Act on the Protection of Personal Information (APPI).

2. For each law and regulation identified in Question 1, please describe:

a. The general scope of the breach notice requirement.

The APPI itself does not provide that breach notification is a mandatory requirement. However, the Guidelines of the Ministry of Economy, Trade and Industry (“METI”) “recommend” that the company make a breach notification when a breach occurs. Further, the Guidelines of the Financial Service Agency provide that it is an obligation for banks and other financial institutions to make a notification when a breach of personal data occurs in banks or other financial institutions.

b. The definition or standard of a covered “data breach.”

The APPI and Guidelines do not have a specific definition of data breach. The Guidelines of METI provide that notification to data subjects may be omitted if there is no likelihood that the data subject would be damaged by the breach, such as when the personal data is highly encrypted. However, the Guidelines provide that a notification should be submitted to the governmental authority even in such a case.

c. Whether it is mandatory to notify affected individuals.

No.

d. Whether it is mandatory to notify any government authorities.

No.

e. Whether any other parties may need to be notified of the incident.

Yes.

There are several industry groups which provide that the member companies have an obligation to make a report to the industry group in addition to the notification to the competent governmental authority.
f. Whether the above rules are different if the company is acting as a data processor/service provider, and not acting as the data controller/owner of the information at issue.

No.

g. What are the potential penalties for non-compliance with the breach notice obligation?

The non-compliance itself would not immediately trigger penalties. Penalties will be applicable when the company does not comply with a specific order from the competent ministry.
1. In your jurisdiction, are there legal requirements for organizations to provide notice of a breach of security for personal data or other company information?

Yes.

**Please identify the name of the relevant law(s) or regulation(s).**

The obligation to provide notice of a breach of security in connection with personal data to the National Commission for the Protection of Personal Data (“CNPD”) is provided by article 3(3) of the law of 30 May 2005, as amended, laying down specific provisions for the protection of persons with regard to the processing of personal data in the electronic communications sector (“loi du 30 mai 2005, telle que modifie, relative aux dispositions specifiques de protection de la personnel gard du traitement des donnes caractre personnel dans le secteur des communications lectroniques”) (the “Law”).

2. For each law and regulation identified in Question 1, please describe:

a. **The general scope of the breach notice requirement.**

The only existing obligation to provide notice of a breach of security is in the sector of electronic communications.

There is no other legal obligation to notify data security breaches. The data controller could, however, always decide, depending on the importance of the breach, to inform the CNPD or the affected individual on a voluntary and purely informative basis, based on an internal management decision and not as a consequence of a legal requirement.

b. **The definition or standard of a covered “data breach.”**

“Data breach” is defined by article 2(m) of the Law as “a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access to, personal data transmitted, stored or otherwise processed in connection with the provision of publicly available electronic communications services.”

This definition includes all sorts of incidents, such as the access by third parties, by way of the internet, to servers containing the customers’ data because of vulnerabilities in the security system of the provider of electronic communications services concerned, or the loss by an employee of a provider of electronic communications services of a CD-ROM or USB stick containing customers’ data.
c. **Whether it is mandatory to notify affected individuals.**
Yes.

It is only mandatory to notify individuals where the data breach is such as to adversely affect the personal data or privacy of a subscriber or individual (article 3(3) of the Law). By way of illustration, a data breach is likely to adversely affect the personal data or privacy of a subscriber or individual occurs, in particular, where the data breach may result in an identity theft, a physical harm, a significant humiliation or damage to reputation in connection with the provision of publicly available communications services.

The notification to the subscriber should be written in a clear and understandable language, and comprise at least the following information:

- the name of the provider;
- the identity and contact details of the data protection officer or any other person from whom more information can be obtained;
- the summary of the incident which has caused the security breach;
- the estimated date of the incident;
- the nature and substance of the personal data concerned;
- likely consequences of the security breach for the subscriber or the individual; circumstances of the security breach; and
- measures taken by the provider to remedy the security breach;
- measures recommended by the provider to mitigate the potential harm.

Nonetheless, the notification to a subscriber or individual is not necessary, if the provider has demonstrated to the satisfaction of the CNPD that it has implemented all appropriate technological protection measures and that those measures were applied to the personal data concerned by the security breach. Such technological protection measures shall render the data unintelligible to any person who is not authorized to access it.

d. **Whether it is mandatory to notify any government authorities.**
Yes.

The providers of electronic communications services should notify the CNPD within 24 hours from the observance of a security and confidentiality breach.

This initial notification should contain the following information:

- the date and time of the incident;
- the nature and substance of the personal data concerned;
circumstances of the security breach;

- technical and organizational measures taken or intended to be taken by
the provider to the personal data concerned; and

- recourse to other providers which have played a role, if any.

As soon as possible, but at the latest 3 days after the initial notification, the
provider shall provide the CNPD with a second notification containing at least
the following information:

- the summary of the incident which has caused the security breach;

- number of subscribers or individuals concerned;

- consequences and potential harms for subscribers and individuals; and

- technical and organizational measures taken by the provider to mitigate
the potential harms.

Providers should maintain an inventory of personal data breaches to enable
further analysis and evaluation by the CNPD.

e. **Whether any other parties may need to be notified of the incident.**

   No.

f. **Whether the above rules are different if the company is acting
as a data processor/service provider, and not acting as the
data controller/owner of the information at issue.**

   Yes.

Although there is no express mention in the applicable law, the obligation to
notify the security breach is traditionally considered as borne by the data
controller which is ultimately liable for the processing of personal data
operated.

g. **What are the potential penalties for non-compliance with the
breach notice obligation?**

   The CNPD alerts the provider regarding its obligation to notify the security
breach where a first failure to comply with the notification obligation occurs. In
case of repeated infringements, the CNPD may pronounce a fine which may
not exceed EUR 50,000.

   Failure to take the appropriate technical and organizational measures in order
to guarantee the security of the services, to inform the subscribers, and to
keep an inventory of personal data breaches are punishable by imprisonment
between 8 days and one year and/or a fine between EUR 251 and EUR
125,000. The judge may also pronounce the cessation of the processing contrary to the provisions of the applicable law, as well as a periodic penalty payment.
Malaysia

Woo Wei Kwang
Kuala Lumpur
Tel: +603 2298 7898
weikwang.woo@WongPartners.com

Shameen Binti Mohd. Haaziq Pillay
Kuala Lumpur
Tel: +603 2298 7943
shameen.mohd.haaziqPillay@WongPartners.com
1. In your jurisdiction, are there legal requirements for organizations to provide notice of a breach of security for personal data or other company information?

No.

2. For each law and regulation identified in Question 1, please describe:

a. **The general scope of the breach notice requirement.**
   In Malaysia, there is no legal requirement at present to notify data subjects or the Personal Data Protection Department (“Regulator”) of a personal data security breach. Therefore, there is no prescribed scope of breach notice requirements.

b. **The definition or standard of a covered “data breach.”**
   There is no definition or standard of data breaches that require notification.

c. **Whether it is mandatory to notify affected individuals.**
   No.
   Even though it is not mandatory to notify affected individuals, data users are advised to do so as a recommended practice for the proper handling of data breaches.

d. **Whether it is mandatory to notify any government authorities.**
   No.
   Even though there is no mandatory reporting obligation to any authority at present, data users are advised to do so as a recommended practice for proper handling of data breaches.

e. **Whether any other parties may need to be notified of the incident.**
   No.

f. **Whether the above rules are different if the company is acting as a data processor/service provider, and not acting as the data controller/owner of the information at issue.**
   No.
   There is no positive obligation placed on a data processor to notify data subjects or the Regulator in the event of a data security breach. Depending, however, on the contractual terms between the data user and the data processor, the data processor may be under a contractual obligation to notify...
the data user of the data security breach and to work together with the data user to rectify the situation.

**g. What are the potential penalties for non-compliance with the breach notice obligation?**

No specific penalties. Contravention of the Security Principle however, by virtue of the data security breach, could amount to an offence. Upon conviction, the penalty is a fine not exceeding RM 300,000 and/or imprisonment for a term not exceeding 2 years.
Mexico

**Sergio Legorreta-Gonzalez**  
Mexico City  
Tel: +52 55 5279 2954  
sergio.legorreta-gonzalez@bakermckenzie.com

**Carlos Vela-Trevino**  
Mexico City  
Tel: +52 55 5279 2911  
carlos.vela-trevino@bakermckenzie.com
1. In your jurisdiction, are there legal requirements for organizations to provide notice of a breach of security for personal data or other company information?

Yes.

Please identify the name of the relevant law(s) or regulation(s).

Our Federal Constitution, The Federal Law of Personal Data Protection in Possession of Particulars, as well as its Regulations, set the liability for protection of personal data, for both Authorities and citizens in case of a breach of security for personal data.

Also, some Federal Institutions aid the INAI (National Institute of Transparency, Access to Information and Protection of Personal Data) in creating additional regulations in different sectors like: Health, Economy, Transportation, Education, and Taxes.

2. For each law and regulation identified in Question 1, please describe:

   a. The general scope of the breach notice requirement.
      
      The scope of the breach notice requirement includes any information concerning an identified or identifiable individual that materially affects their property or moral rights.

   b. The definition or standard of a covered “data breach.”
      
      A data breach consists of the following:
      (i) the loss or unauthorized use of personal data;
      (ii) the stealing or unauthorized copying of data;
      (iii) misuse or unauthorized treatment of data; and
      (iv) the unauthorized alteration of data.
      
      These actions will not be considered as breach, if an Authority requires such information for a trial, and/or audit.

   c. Whether it is mandatory to notify affected individuals.
      
      Yes.
      
      The responsible entity must send a notification to the data owner: (i) as soon as the controller has confirmed that a security breach has occurred; and (ii) the controller has taken action which may lead to a more in-depth assessment to determine the magnitude of the breach. In any case, these internal
procedures must be conducted without unnecessary delay, so that notification to affected individuals may be provided promptly and they may take appropriate action.

d. Whether it is mandatory to notify any government authorities. No.
e. Whether any other parties may need to be notified of the incident. Yes.

It is possible that several third parties were affected as well, so the responsible entity must notify the affected individuals of such data breach.

f. Whether the above rules are different if the company is acting as a data processor/service provider, and not acting as the data controller/owner of the information at issue. No.

g. What are the potential penalties for non-compliance with the breach notice obligation?

First, the Authority mandates the responsible entity comply with the requirements of the law in terms of its obligations to the data owner in the event of a breach. Otherwise, a fine may be imposed for as high as 320,000 times the minimum current salary. Also if this breach is caused in pursuance of an economic benefit affecting the owner’s rights and security, the penalty is imprisonment of up to 5 years, if non-sensitive personal data is involved, or 10 years if sensitive data is involved.
Netherlands

Wouter Seinen
Amsterdam
Tel: +31 20 551 7161
wouter.seinen@bakermckenzie.com

Silvia van Schaik
Amsterdam
Tel: +31 20 551 7146
silvia.vanschaik@bakermckenzie.com
1. In your jurisdiction, are there legal requirements for organizations to provide notice of a breach of security for personal data or other company information?

Please identify the name of the relevant law(s) or regulation(s).

A general requirement to provide a notice of breaches of data security applies to breaches involving personal data processed by or on behalf of a data controller that is subject to the Dutch data protection act ("PDPA", in Dutch: Wet bescherming persoonsgegevens):

- Articles 27, 28, 33 and 34 PDPA, and, in particular, (per 1-1-2016) Article 34(a) PDPA.

Providers of publicly available electronic communications services ("ISPs") are required to provide notice to their regulator of data breaches involving data processed in the course of their provision of service;

- Article 11.3(a), 11a.2 and 14.6 Telecommunications Act ("TA", in Dutch: Telecommunicatiewet)

Regulated financial institutions are required to notify data breaches to their regulators, in particular when the data breach in question may potentially have an adverse impact on the stability of the financial services sector;

- Article 3.10(3), 4.11(4) and 5.25(i) Financial Supervisory Act ("FSA", in Dutch: Wet op het financieel toezicht);

- Article 12.3 Decree on Prudential Rules for Financial Undertakings (in Dutch: Besluit prudentiële regels Wft);

- Article 19 Decree on Conduct of Business Supervision of Financial Undertakings under the Wft (in Dutch: Besluit Gedragstoezicht financiële ondernemingen Wft)

2. For each law and regulation identified in Question 1, please describe:

a. The general scope of the breach notice requirement.

Personal Data Protection Act

The PDPA applies to the processing of personal data by or on behalf of an organization that is established in the Netherlands or processes personal data in the course of an establishment in the Netherlands.

Effective 1 January 2016, a data security breach includes an incident: (i) that has or is likely to have serious adverse consequences for the protection of personal data; and (ii) when there is reason to believe that the breach could
have adverse consequences on the privacy of any person whose personal data is concerned (data subjects).

On a more general note, data controllers (the persons or entities that determine the purpose of and means for processing personal data) have to provide their data subjects with information relating to the processing of their personal data and inform them of transfers of their personal data to others. This means that, when a data breach is likely to have caused others to access the data, this is already considered to fall under the general information requirements under the PDPA prior to 2016. However, this was not enforced or otherwise given much attention prior to the data breach notification duty specifically introduced in the PDPA.

Insofar as data breaches involving data processing operations subject to the specific data breach notifications under the Telecommunications Act are concerned (see below), the notification requirements under the PDPA do not apply.¹

**Telecommunications Act**

Article 11.3(a) of the Telecommunications Act (“TA”) provides a data breach notification requirement that applies to all ISPs providing services in the Netherlands. In order to protect the personal data and privacy of subscribers and users of their services, the providers are obliged to put security measures in place. The breach notice obligation is restricted to breaches that have an adverse impact on the protection of the personal data processed in the course of the telecommunications services rendered. To the extent that a breach is likely to have an adverse impact on the privacy of certain data subjects, the ISP is also required to notify such affected customers.

Another notice obligation relating to the continuity of public electronic communications networks or services can be found in Article 11a.2. This obligation applies to all providers of publicly available electronic communications services and providers of public electronic communications networks. The notice obligation is required for: (i) breaches of security; and (ii) loss of integrity, which cause, to a considerable degree, the obstruction of the continuity of the networks or services.

**Financial Supervisory Act**

There are two general notification requirements under the Financial Supervisory Act (“FSA”).

According to Article 3.10(3), a clearing institution, credit institution or insurer having its registered office in the Netherlands shall implement an adequate

¹ See Article 33 and 34 of the DPA.
policy that safeguards controlled and sound business operations. Accordingly, these institutions will have to take measures to, for instance, prevent the financial institution or its employees from committing offences that could damage public trust in the institution at hand or in the financial market in general.

The same obligation can be found in Article 4.11(4) for management companies, investment companies, investment firms or depositaries.

The two additional decrees to the FSA, Decree on Prudential Rules for Financial Undertakings and the Decree on Conduct of Business Supervision of Financial Undertakings under the Wft also require the institutions subject to these decrees to notify any events that could damage the controlled and sound business operations. The obligations laid down in these Decrees are implemented in the FSA and will not be discussed separately.

Furthermore, Article 5.25i of the FSA includes the obligation for financial institutions to notify a communication of insider information to ensure an adequate policy that safeguards controlled and sound business operations. Insider information means specific information that relates directly or indirectly to an issuer to which the financial instruments pertain, or to the trade in those financial instruments, with information that has not been publicly disclosed and whose disclosure might have a significant influence on the price of the financial instruments or on the price of derivative financial instruments.

As of 1 January 2016, financial institutions are also required to notify breaches which lead to a significant probability of serious detrimental consequences for the protection of personal data. This obligation is, however, restricted in scope; the exceptions are detailed below.

b. The definition or standard of a covered “data breach.”

Personal Data Protection Act

Under the personal data breach notification duty of article 34a PDPA, a data breach is understood to mean any breach on the organizational and technical measures to protect personal data against loss, integrity issues and unauthorized access. The following are considered to be examples of breaches: an email that was occasionally sent to a group of users in open cc rather than to undisclosed recipients; the loss of a password; a user authorization of an ex employee not being revoked on termination; and the loss of a smartphone.

Not all “breaches” have to be notified, however. For instance, when the data controller has taken appropriate technical protective measures to ensure that data is unintelligible or inaccessible for third parties, for example by
encryption.\textsuperscript{2} Similarly, if a laptop was destroyed or a system crashed, there may be copies of data lost, but if the same data can be retrieved from a backup, there is no loss of data that can have adverse impact. If a laptop was stolen but wiped remotely or properly encrypted (and not accessible when it was stolen), the data breach is not subject to the notification duty.

\textbf{Telecommunications Act}

Under the TA, data breach is defined as:

“a security breach resulting in an accidental or unlawful destruction, loss or alteration of, or unauthorized access to personal data transmitted, stored or otherwise processed in connection with the provision of a publicly available electronic communications service within the European Union.”

Notification to the parties whose personal data are concerned is not required if the Authority Consumers and Markets (“ACM”) considers that the provider has taken appropriate technical protective measures such as encrypting the data or making them otherwise incomprehensible.

\textbf{Financial Supervisory Act}

Under the FSA, the notice obligation applies to breaches of the following conducts or events which pose a serious threat to the sound conduct of the financial institution’s business:

(a) measures are taken to prevent conflicts of interest;

(b) measures are taken to prevent the financial enterprise or its employees from committing offences or other transgressions of the law that could damage confidence in the financial enterprise or in the financial markets;

(c) measures are taken to prevent confidence in the financial enterprise or in the financial markets from being damaged because of its clients; and

(d) measures are taken to prevent the financial enterprise or its employees from performing other acts that are so contrary to generally accepted standards as to seriously damage confidence in the financial enterprise or in the financial markets.

\textbf{c. Whether it is mandatory to notify affected individuals.}

\textbf{Personal Data Protection Act}

Under the new article 34a PDPA (effective 1 January 2016), data controllers are obliged to “immediately” notify the individuals whose personal data are

\footnote{2 Article 34a(6) of the DPA.}
compromised when there is reason to believe the breach is capable of resulting in adverse consequences for their privacy.

The notice to the affected data subjects should contain information regarding:

(i) the nature of the breach;
(ii) the bodies that can provide further information on the breach; and
(iii) proposed measures to mitigate the adverse consequences of the breach.

Article 34a of the PDPA does not include a standard for timing of the notification but “immediately” can be understood as “without delay.” The Dutch DPA has issued Guidelines pursuant to which a notification must be submitted within two business days from the moment the data breach was discovered.

The notification obligation is not applicable in case the data controller, being a provider of public electronic communications services, has notified the breach in accordance with Article 11.3a of the TA.

**Telecommunications Act**

Data subjects must be informed if the data breach is **likely** to have unfavourable consequences for the data subject’s privacy.

The notification to the data subject’s shall contain information on:

(i) the nature of the breach;
(ii) the bodies from which more information can be acquired regarding the breach and
(iii) the recommended measures to mitigate the negative consequences of the breach.

Notification must be made ‘immediately’. According to the Dutch Telecom Agency (**Agentschap Telecom**) notification within 24 hours after the breach has been discovered is sufficient. However, there is no legal time notification requirement under the TA.

In case the service provider fails to notify data subjects, the ACM may require notification after all if the breach, in connection with personal data, is likely to have unfavourable consequences for the personal privacy of that party.

**Financial Supervisory Act**

Following the FSA, financial institutions are, in principle, not required to inform the affected parties. Nonetheless, the duty of care arising out of these articles, implicates an indirect notification obligation in case of incidents that pose a serious threat to the sound conduct of the financial institution’s business. According to the Explanatory Memorandum to the FSA, this duty of care
provides a sufficient guarantee that financial institutions contact their clients directly.

As of January 2016, financial organisations falling under the FSA are explicitly exempt from having to notify the affected data subjects.3

d. Whether it is mandatory to notify any government authorities.

Personal Data Protection Act

Pursuant to the data breach notification duty effective on 1 January 2016, data controllers will have to provide, in addition to the information that has to be provided to the affected data subjects, the following information to the Dutch DPA:

(i) technical details and background of the breach; and

(ii) expected consequences of the data breach to the processing of personal data and the measures taken by the data controller to tackle those consequences.

Article 34a of the PDPA does not include a standard for timing of the notification but “immediately” can be understood as “without delay.” The Dutch DPA has issued Guidelines pursuant to which a notification must be submitted within two business days from the moment the data breach was discovered.

The notification obligation is not applicable in case the data controller, being a provider of public electronic communications services, has notified the breach in accordance with Article 11.3a of the TA.

Telecommunications Act

The TA requires providers of a publicly available electronic communications service to notify the ACM immediately of any breach of security that has negative consequences for the protection of personal data processed in connection with the provision of a publicly available electronic communications service within the European Union.

The notification to the ACM shall comprise the same aspects as required for the notification to affected data subjects plus:

(i) the consequences of the breach for the personal data; and

(ii) the measures that the provider proposes or has taken in order to deal with the breach.

There is no legal standard for the timing of the notification as mentioned before, other than the fact that it must be made “immediately.”

3 See Article 34a(10) of the DPA.
It is important to note that, as of January 2016, providers falling under the TA will have to notify the Dutch DPA instead of the ACM.

Financial Supervisory Act

Financial organisations falling under the FSA are required to provide information relating to the relevant conduct or event under Articles 3.10(3) and 4.11(4) to the Authority Financial Markets “AFM.”

As of January 2016, financial institutions that process personal data, hence acting as data controllers, have to notify the Dutch DPA of a data security breach.

With regard to situations in which inside information is leaked, the institution has to publicly disclose the information immediately after reporting to the AFM.\(^4\)

e. Whether any other parties may need to be notified of the incident.

No

f. Whether the above rules are different if the company is acting as a data processor/service provider, and not acting as the data controller/owner of the information at issue.

Personal Data Protection Act

Only data controllers are subject to the data breach notification duty. Data controllers may be required to notify their customers (data controllers that are subject to the PDPA) under contractual obligations, but they are not under a statutory obligation to notify.

The notification duty does, however, extend to data processors in foreign countries that process data for Dutch controllers. It is up to the controller to ensure that they are timely informed of any data breaches taking place in the processing operation of a (foreign) processor.

Telecommunications Act

The TA does not distinguish between controllers and processors. Only providers of public electronic communications services have to notify the ACM (as of January 2016 to the DPA) of any security breaches.

\(^4\) See Article 5.25i(5) of the FSA.
Financial Supervisory Law

The rules relating to breach notice obligations under the FSA do not depend on the distinction between controllers and processors of personal data.

g. What are the potential penalties for non-compliance with the breach notice obligation?

Data Protection Act

As per January 2016, the maximum fines for violations of the PDPA amount to EUR 810,000- or 10% of the company’s annual net turnover. These fines also cover violations of data breach notification duties and non-compliance with their obligation under Article 5.20 of the Dutch General Administrative Act to cooperate with the supervisory authorities in the exercise of their information-gathering powers. However, it is expected that the Dutch DPA may impose fines of EUR 120,000 - EUR 500,000 for failure to timely and correctly notify a data breach.

Telecommunications Act

The ACM has powers to impose fines of up to EUR 450,000- for non-compliance with the security breach notification obligation laid down in Article 11.3a of the TA. In addition, the ACM is entitled to impose similar fines for failure to cooperate in an investigation pursuant to Article 5.20 of the Dutch Administrative Law. To enhance expedience of the different notification obligations laid down in the PDPA and the TA, the Dutch DPA also have the authority to impose fines on providers falling under the TA as of January 2016.

Financial Supervisory Act

Fines for breaches of the FSA can vary between EUR 10,000- and 5,000,000.

---

5 See Article 66 of the amended DPA in relation to Article 5.20 of the Dutch General Administrative Act.
6 See Explanatory Memorandum to the bill, para. 4.1.
7 See Article 1.81 of the FSA.
New Zealand

Karen Ngan
Auckland
Tel: +64 9 977 5080
karen.ngan@simpsongrierson.com

Carl Blake
Auckland
Tel: +64 9 977 5163
carl.blake@simpsongrierson.com
1. Overview

The key legislation governing privacy and data collection in New Zealand is the Privacy Act 1993 ("Privacy Act"). The Privacy Act sets out a number of Information Privacy Principles ("IPPs") that govern the collection, storage and security, accuracy, retention, use and disclosure of personal information. Personal information is defined in the Privacy Act as information about an identifiable individual, defined as a natural person (other than a deceased natural person) and includes information relating to a death that is maintained by the Registrar-General pursuant to the Births, Deaths, Marriages and Relationships Act 1995 ("BDMRA") or any former Act (as defined by the BDMRA). The Privacy Act applies to "agencies," including Government, private sector businesses, voluntary sector and non-government organisations.¹

2. Privacy Breach Guidelines

New Zealand does not currently have mandatory data security breach notification requirements. However, the New Zealand Privacy Commissioner (Privacy Commissioner) has issued voluntary guidelines to assist agencies to respond to data security breaches (Privacy Breach Guidelines).²

The Privacy Breach Guidelines are intended to assist agencies to plan in advance for a breach and to ensure that they are prepared to manage breaches successfully, for the benefit of the agency and affected individuals. A key step under the Privacy Breach Guidelines is notification to the Privacy Commissioner and/or the affected individuals. Agencies are encouraged to notify the Privacy Commissioner of material privacy breaches so his office is aware of the breach and able to effectively handle inquiries or complaints. Whether or not affected individuals should also be notified involves consideration of whether notification is necessary to avoid or mitigate harm to the individual. The Privacy Breach Guidelines set out a number of factors to consider when deciding to notify. These include:

- What are the legal and contractual obligations?
- What is the risk of harm to the individual?

¹ Privacy Act 1993, s 2. There are a number of limited exceptions including the Sovereign, Governor-General, a court or tribunal in carrying out its judicial functions, an ombudsman or commission of inquiry and a news medium in relation to its new activities.


Baker & McKenzie
• Is there a reasonable risk of identity theft or fraud?
• Is there a risk of physical harm?
• Is there a risk of sufficient humiliation or loss of dignity, damage to reputation or relationships?

In addition to the Privacy Breach Guidelines, the Privacy Commissioner has a Naming Agencies in Public Reports Policy\(^3\) - often referred to as a “name and shame” policy. This policy records the Privacy Commissioner’s willingness to publically name agencies that have breached the Privacy Act.

3. Penalties for Data Security Breach

As there is no current requirement for mandatory data security breach notification, there are no specific fines or penalties for failing to notify. However, a data security breach could give rise to a claim that there has been an interference with privacy. This could result in the Privacy Commissioner investigating the complaint and seek to secure a settlement. If this is unsuccessful, the matter could become the subject of proceedings before the Human Rights Review Tribunal (“Tribunal”) issued by the Director of Human Rights Proceedings or by the aggrieved individual. The Tribunal has jurisdiction to make awards of up to $200,000, with the highest damages awarded by the Tribunal to date being $168,070.88, awarded in Hammond v Credit Union Baywide [2015] NZHRRT 6. The previous highest award by the Tribunal in respect of a claim made under the Privacy Act was $40,000.

4. Privacy Reform – Mandatory Data Breach Notification

Following recommendations arising from the 2011 Law Commission review into the Privacy Act,\(^4\) the Government has signalled its intent to repeal and replace New Zealand’s existing privacy law regime, however a draft Privacy bill has not been released. A 2014 Cabinet Paper issued by the Cabinet Social Policy Committee (“Cabinet Paper”)\(^5\) suggests that mandatory reporting of data breaches will be one of the major reforms introduced under the new legislation.

\(^5\) Cabinet Social Policy Committee “Reforming the Privacy Act 1993” (13 March 2014).
a. **Notification Requirements**

The Cabinet Paper indicates that a two tier approach may be adopted for the notification of privacy breaches. Notification is expected to be required for:

- Tier 1 – “material” breaches; and
- Tier 2 – “serious” breaches.

It is anticipated that the Privacy Commissioner would need to be notified of both tier 1 and tier 2 breaches and that tier 2 breaches may also have to be notified to affected individuals where there is a “real risk of harm.” Precisely what will be considered a “material” or “serious” breach is unclear. The Cabinet Paper indicates that notifiable “serious” breaches where there is a “real risk of harm” are likely to involve actual or potential loss, injury, significant humiliation, or adverse effects on rights or benefits.

b. **Potential penalties for non-compliance**

It is also anticipated that the proposed reforms will see the introduction of fines for failing to comply with the new mandatory data breach notification requirement. The level of the fine is not confirmed but indications are that it could be up to $10,000.
Norway

Espen Sandvik
Oslo
Tel: +47 98 29 45 41
esa@adeb.no

Cato Lower
Oslo
Tel: +47 98 29 45 15
clo@adeb.no
1. In your jurisdiction, are there legal requirements for organizations to provide notice of a breach of security for personal data or other company information?

Yes.

Please identify the name of the relevant law(s) or regulation(s).

- The Personal Data Act,
- The Personal Data Regulations

2. For each law and regulation identified in Question 1, please describe:

a. The general scope of the breach notice requirement.

Neither the Personal Data Act nor the Personal Data Regulations explicitly prescribe that it is mandatory to notify affected individuals in the event of a data breach. A strong argument could nevertheless be made that such a notification obligation lies implicit in the Personal Data Act and its purpose. The Norwegian Data Inspectorate has also explicitly stated that there is a notification requirement in case of data breach that could be “harmful” for the affected individual. An omission to notify the affected individual could also entail liability pursuant to tort law, if a notification would have reduced the damage of the affected individual. To be on the safe side, we therefore strongly recommend that affected individuals are notified in the event of a data breach that could be “harmful” to them. The Norwegian Data Inspectorate has stated that the following elements are important in the evaluation of whether the affected individual must be notified:

(i) the risk of physical damage (physical injuries, harassment, stalking);
(ii) risk of identity theft or forgery (which is dependent on the information lost);
(iii) the risk of damage to the affected individual’s reputation; and
(iv) the affected individual’s opportunity to avoid or limit the damage by the breach (are the information trade secrets, etc.).

Based on these elements, it would typically be a data breach of sensitive personal data (health, credit card numbers etc.) that would be “harmful.” The notification requirements apply to all sectors. The Norwegian Data Inspectorate shall be notified “If the discrepancy has resulted in the unauthorized disclosure of personal data where confidentiality is necessary,” pursuant to Section 2-6 of the Personal Data Regulations. Personal data where “confidentiality is necessary” will typically be sensitive personal data.
(personal identification number, credit card number, religion etc.). The obligation to notify the Norwegian Data Inspectorate applies to all sectors in principle.

b. **The definition or standard of a covered “data breach.”**

A “data breach” pursuant to the Personal Data Act is when unauthorized people or enterprises get access to the personal data. It is our view that there are no exceptions from the notification obligation if the conditions above in 2(a) are present.

c. **Whether it is mandatory to notify affected individuals.**

Yes.

According to the Norwegian Data Inspectorate, notification to affected individuals should be carried out as soon as possible after the data breach (provided that the data breach could be “harmful” to the individual). If the police or other governmental authorities are involved, it is important to consult with them prior to any notification (to avoid harming an on-going investigation). The notification to the affected individual should happen directly by telephone, letter, email or personal notification. Indirect notification (on website, media etc.) should be chosen when direct notification could be harmful to the affected individuals involved, direct notification would be very costly or if the contact information of the affected individual is unknown.

d. **Whether it is mandatory to notify any government authorities.**

Yes.

Notification shall be sent to the Norwegian Data Inspectorate (provided that the conditions in Section 2-6 of the Personal Data Regulations are met). The notification should include:

(i) a description of the data breach;

(ii) what kind of personal data that has been lost;

(iii) the risk that the personal data is used for identity theft, economic crimes etc.; and

(iv) the number of affected individuals.

If any of the affected individuals have been notified. It is also the Norwegian Data Inspectorate’s recommendation to consider whether it is necessary to notify the Police, insurance companies, credit card companies etc., which may have an interest in being informed of the data breach.

e. **Whether any other parties may need to be notified of the incident.**

No.
f. Whether the above rules are different if the company is acting as a data processor/service provider, and not acting as the data controller/owner of the information at issue.

No.

g. What are the potential penalties for non-compliance with the breach notice obligation?

There are several potential penalties for non-compliance with the breach notice obligation: The Personal Data Act Section 46 prescribes that “The Data Inspectorate may issue orders to the effect that violation of provisions laid down in or pursuant to this Act shall result in a fine to the Treasury (Data Offence Fine) of maximum 10 times the National Insurance Basic Amount” (around EURO 100.000,-). In addition, it follows from Section 49 of the Personal Data Act that “The controller shall compensate damage suffered as a result of the fact that personal data have been processed contrary to provisions laid down in or pursuant to this Act, unless it is established that the damage is not due to error or neglect on the part of the controller. Controllers who provide credit information and who have communicated information which proves to be inaccurate or obviously misleading shall compensate any damage that has been suffered as a result of the erroneous communication, regardless of whether the damage is due to error or neglect on the part of the controller. The compensation shall be equivalent to the financial loss incurred by the injured party as a result of the unlawful processing. The controller may also be ordered to pay such compensation for damage of a non-economic nature (compensation for non-pecuniary damage) as seems reasonable.” It follows from Section 10-3 of the Personal Data Regulations that “Anyone who willfully or through gross negligence omits to comply with the provisions of chapters 2 [including the notification obligation to the Norwegian Data Inspectorate pursuant to Section 2-6] shall be liable to fines or imprisonment for a term not exceeding one year or both. An accomplice shall be liable to similar penalties.”
Peru

**Javier Tovar**  
Lima  
Tel: +51 1 618 8500 Ext. 550  
javier.tovar@bakermckenzie.com

**Teresa Tovar**  
Lima  
Tel: +51 1 618 8500 Ext. 552  
teresa.tovar@bakermckenzie.com

**Viviana Chavez**  
Lima  
Tel: +51 1 618 8500 Ext. 421  
viviana.chavez@bakermckenzie.com
1. In your jurisdiction, are there legal requirements for organizations to provide notice of a breach of security for personal data or other company information?

Yes.

Please identify the name of the relevant law(s) or regulation(s).

Even though neither the Data Protection Law (Law No. 29733) and its Regulation (approved through Supreme Decree No. 003-2013-JUS) contain a provision which provides that notice of a breach of security is mandatory, both oblige the holder of a data bank (and processor, if its the case) to implement security measures to prevent the unauthorized access to personal data. As a consequence, an implied obligation would be to adopt all corrective measures in the event of a data breach to minimize the damages it may cause to the data subjects.

In addition, a Security Directive approved by the Peruvian Data Protection Authority through Directorial Resolution No. 019-2013-JUS/DGPDP (not mandatory, but recommended in order to comply with the general duty of security) states that any case of data breach should be informed to the data subjects as soon as it is confirmed.

2. For each law and regulation identified in Question 1, please describe:

a. The general scope of the breach notice requirement.

There are no provisions on this regard.

b. The definition or standard of a covered “data breach.”

The Security Directive recommends notification of data breaches that significantly affect the economic and/or moral rights of the data subjects.

c. Whether it is mandatory to notify affected individuals.

Yes.

Neither the Law nor the Regulation contains provisions on this regard. However, the Security Directive does recommend notifying individuals. It states that the minimum information to be provided to the individual is as follows:

- Nature of the incident;
- Personal data involved in the data breach;
- Recommendations to the data subject; and
• Corrective measures implemented.

d. Whether it is mandatory to notify any government authorities. No.
e. Whether any other parties may need to be notified of the incident. No.
f. Whether the above rules are different if the company is acting as a data processor/service provider, and not acting as the data controller/owner of the information at issue. Yes.

The entity responsible for adopting security measures and notifying individuals of a data breach is the entity responsible for the processing (that is to say, the holder of the data bank and the processor, if it is the case).

g. What are the potential penalties for non-compliance with the breach notice obligation?

The non-compliance of the security duty (which may include not adopting the corresponding measures to minimize the risks of a data breach) are sanctioned with fines. The level of the fine would depend on the gravity of the case. However, please note that the Data Protection Authority is entitled to impose fines of up to 100 Tax Units (US$ 128,000.00, approximately). Also, the Data Protection Authority can order corrective measures (adopt actions to minimize the risks, which include informing data subjects of the incident and providing them with security recommendations).
Philippines

Bienvenido Marquez
Manila
Tel: +63 2 819 4936
bienvenido.marquez@quisumbingtorres.com

Divina Ilas-Panganiban
Manila
Tel: +63 2 819 4961
divina.ilas-panganiban@quisumbingtorres.com
1. In your jurisdiction, are there legal requirements for organizations to provide notice of a breach of security for personal data or other company information?

Yes.

Please identify the name of the relevant law(s) or regulation(s).

Republic Act no. 10175, otherwise known as the Data Privacy Act of 2012 ("DPA"), Republic Act No. 10173, otherwise known as the Cybercrime Prevention Act of 2012, Bangko Sentral ng Pilipinas ("BSP") Circular No. 808 - Guidelines on Information Technology Risk Management for All Banks and Other BSP Supervised Institutions.

2. For each law and regulation identified in Question 1, please describe:

a. The general scope of the breach notice requirement.

Under Sec. 20 (f) of the DPA, the breach notice requirement of a Personal Information Controller ("PIC") applies when sensitive personal information or other information that may, under the circumstances, be used to enable identity fraud are reasonably believed to have been acquired by an unauthorized person, and that such unauthorized acquisition is likely to give rise to a real risk of serious harm to any affected data subject.

The notification shall at least describe the nature of the breach, the sensitive personal information possibly involved, and the measures taken by the entity to address the breach. 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.

Moreover, §X176.8 (2) of BSP Circular No. 808 requires BSP supervised institutions ("BSI") to submit a report on the breach in information security, especially incidents involving the use of electronic channels, pursuant to the provisions of the Manual of Regulations for Banks following the guidelines on reporting on crimes / loses. Depending on the nature and seriousness of the incident, the BSP may require the BSI to provide further information or updates on the reported incident until the matter is finally resolved.

1 The Bangko Sentral has supervision over the operations of banks and exercises such regulatory powers as provided in the New Central Bank Act and other pertinent laws over the operations of finance companies and non-bank financial institutions performing quasi-banking functions.
Outsourcing contracts also require that the BSI ensure the service providers’ physical and data security standards meet or exceed the BSI’s standards, and any breach in security should be reported by the service provider to the BSI.

b. **The definition or standard of a covered “data breach.”**

The following are exceptions to the obligation to notify:

(1) In evaluating if notification is not required, the National Privacy Commission (“NPC”) may take into account compliance by the PIC of its obligation to notify data breaches and existence of good faith in the acquisition of personal information.

(2) The NPC may exempt a PIC from notification where, in its reasonable judgment, such notification would not be in the public interest or in the interests of the affected data subjects.

(3) The NPC may authorize postponement of notification where it may hinder the progress of a criminal investigation related to a serious breach.

Note that there are no exceptions in relation to the covered “data breach” under the BSP Circular No. 808.

c. **Whether it is mandatory to notify affected individuals.**

Yes.

There is no standard timing, but 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 / communication systems.

d. **Whether it is mandatory to notify any government authorities.**

Yes.

The DPA requires that the NPC and the affected data subject be promptly notified of any incidents of data breaches (in relation to scope described in 2.a above).

Breaches under BSP guidelines need to be reported to the BSP.

e. **Whether any other parties may need to be notified of the incident.**

No.

f. **Whether the above rules are different if the company is acting as a data processor/service provider, and not acting as the data controller/owner of the information at issue.**

Yes.
The above rules may not apply to a company acting as a personal information processor, or those to whom a PIC has outsourced the processing of personal data pertaining to a data subject. The requirement to notify the NPC is the responsibility of the PIC.

However, the law also requires a personal information processor ("PIP", i.e., an entity to whom the PIC may outsource the processing of data) to comply with all the requirements of the DPA and other applicable laws.

Further, pursuant to the DPA’s Principle of Accountability, the PIC should use “contractual or other reasonable means” (See 21 [a] of the DPA) to ensure that the PIP complies with the requirements of the DPA regarding the security of personal information. The PIC should therefore make sure that contractual safeguards are in place for the PIC to be able to comply with the DPA’s notification requirements, such as (i) an agreement for the PIP to immediately inform the PIC whenever personal data breaches occur; and (ii) liquidated damages for failure to report data breaches.

Note that this is more explicit under the BSP guidelines as breaches in security should be reported by the service provider (PIP) to the BSI (PIC).

**g. What are the potential penalties for non-compliance with the breach notice obligation?**

The penalty of imprisonment of one year and six months to five years and a fine of not less than approximately US$10,606.70, but not more than US$21,213.41, shall be imposed on persons who, after having knowledge of a security breach and of the obligation to notify the Commission pursuant to Section 20 (f), intentionally or by omission conceal the fact of such security breach.

BSIs failure to comply with reportorial / notification requirements will subject them to monetary and non-monetary sanctions provided under Section 37 of Republic Act No. 7653 (the New Central Bank Act), including suspension/revocation of authority to provide electronic products and services and prohibition against offering/provision of new electronic products and services.
Poland

Radosław Nożykowski
Warsaw
Tel: +48 22 445 3210
radoslaw.nozykowski@bakermckenzie.com

Magdalena Kogut-Czarkowska
Warsaw
Tel: +48 22 445 3452
magdalena.kogut-czarkowska@bakermckenzie.com
1. In your jurisdiction, are there legal requirements for organizations to provide notice of a breach of security for personal data or other company information?

Yes.

**Please identify the name of the relevant law(s) or regulation(s).**

Act of 16 July 2004 on Telecommunications Law

2. For each law and regulation identified in Question 1, please describe:

a. **The general scope of the breach notice requirement.**

The requirement applies to providers of publicly available telecommunications services.

b. **The definition or standard of a covered “data breach.”**

Data breach is understood as accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data which is processed by a telecommunications undertaking in connection with the provision of publicly available telecommunications services.

c. **Whether it is mandatory to notify affected individuals.**

Yes.

The requirement to notify the affected individuals applies, if the data breach may have adverse effect on the rights of a subscriber or an end user who is a natural person. A personal data breach which may have adverse effect on the rights of a subscriber or end user who is a natural person, means a breach which in particular may result in unauthorized use of personal data, damage to property, breach to personal interests, disclosure of a bank secret or other professional secret protected by law. The notification should be done without delay, not later than within 3 days of finding the breach. The should include: 1) description of the nature of a personal data breach; 2) contact data of a provider of publicly available telecommunications services in order to obtain information about a personal data breach; 3) information about recommended measures intended to mitigate potential adverse effects of a personal data breach; 4) information about the measures undertaken by a provider of publicly available telecommunications services; 5) description of effects of a personal data breach; and 6) description of remedies proposed by a provider of publicly available telecommunications services.
d. **Whether it is mandatory to notify any government authorities.**

Yes.

Data breach must be notified to Inspector General for Personal Data Protection ("GIODO") without delay. The notification should include in particular: 1) description of the nature of a personal data breach and assumed risk related to that breach; 2) contact data of the provider of publicly available telecommunications services in order to obtain information about a personal data breach; 3) information about recommended measures intended to mitigate potential adverse effects of a personal data breach; 4) information about the measures undertaken by the provider of publicly available telecommunications services; 5) information about whether a subscriber or an end user who is a natural person have been informed or not of a personal data breach; 6) description of effects of a personal data breach; 7) description of remedies proposed by the provider of publicly available telecommunications services.

**e. Whether any other parties may need to be notified of the incident.**

No.

**f. Whether the above rules are different if the company is acting as a data processor/service provider, and not acting as the data controller/owner of the information at issue.**

No.

**g. What are the potential penalties for non-compliance with the breach notice obligation?**

Non-compliance with the breach notice obligation may be subject to fines issued by the President of the Office of Electronic Communications (UKE) in the amount of up to 3% of the revenues of a fined entity for the past calendar year. President of UKE may also impose a financial penalty on a person in charge of a telecommunications undertaking, in particular a person performing managerial functions or a member of a management body of that telecommunications undertaking or of an association of such undertakings, up to 300% of his/her monthly remuneration.
Portugal

César Bessa Monteiro
Lisbon
Tel: 351 213 264 747
cesar.bmonteiro@pbbr.pt

César Bessa Monteiro, Jr.
Lisbon
Tel: 351 213 264 747
c.monteiro@pbbr.pt

Ricardo Henriques
Lisbon
Tel: 351 213 264 747
ricardo.henriques@pbbr.pt
1. In your jurisdiction, are there legal requirements for organizations to provide notice of a breach of security for personal data or other company information?

Yes.

Please identify the name of the relevant law(s) or regulation(s).

Law No 41/2004, of 18 August, as amended by Law no. 46/2012, of 29 August, concerning the processing of personal data and the protection of privacy in the electronic communications sector.

2. For each law and regulation identified in Question 1, please describe:

a. The general scope of the breach notice requirement.

The breach notice requirement applies only to providers of publicly available electronic communications services.

b. The definition or standard of a covered “data breach.”

Providers of publicly available electronic communications services shall, without undue delay, notify the personal data breach to CNPD (Portuguese Data Protection Authority).

Where the personal data breach is likely to adversely affect the personal data of the subscriber or user, providers of publicly available electronic communications services shall also notify the subscriber or user of the breach, without undue delay, in order to allow them to take the necessary precautions.

A personal data breach should be considered as adversely affecting the data privacy of a subscriber or user where it could result in, for example, identity theft or fraud, physical harm, significant humiliation or damage to reputation in connection with the provision and use of publicly available communications services.

Notification to subscriber or user shall not be required where providers of publicly available electronic communications services demonstrate to the satisfaction of CNPD that they implemented appropriate technological protection measures, and that those measures were applied to the data concerned by the security breach.

Even when a notification obligation to subscribers or users does not apply, CNPD may require provider to execute such notification, having considered the likely adverse effects of the breach.
c. Whether it is mandatory to notify affected individuals.
Yes.
The law states that the notification shall be “without undue delay.”

d. Whether it is mandatory to notify any government authorities.
Yes.
The authority is CNPD - Comisso Nacional de Proteco de Dados (Portuguese Data Protection Authority). The law states that the notification shall be “without undue delay.”

e. Whether any other parties may need to be notified of the incident.
No.

f. Whether the above rules are different if the company is acting as a data processor/service provider, and not acting as the data controller/owner of the information at issue.
No.

g. What are the potential penalties for non-compliance with the breach notice obligation?
The infringement of the notification obligation amounts to an administrative offense punishable with a fine ranging from a minimum of EUR 1,500 up to EUR 25,000, where committed by natural persons, and from EUR 5,000 up to EUR 5,000,000, where committed by legal persons. The non-compliance with the notification specific requirements is punishable with a fine ranging from a minimum of from EUR 500 up to EUR 20,000, where committed by natural persons, and from EUR 2,500 up to EUR 2,500,000, where committed by legal persons.
Russia

Edward Bekeschenko
Moscow
Tel: +7 495 787 2700
edward.bekeschenko@bakermckenzie.com

Vadim Perevalov
Moscow
Tel: +7 495 787 2700
vadim.perevalov@bakermckenzie.com

Ekaterina Sorokina
Moscow
Tel: +7 495 787 2700
Ekaterina.sorokina@bakermckenzie.com

Dmitry Lysenko
Moscow
Tel: +7 495 787 2700
dmitry.lysenko@bakermckenzie.com
1. In your jurisdiction, are there legal requirements for organizations to provide notice of a breach of security for personal data or other company information?

Under Russian law, there is no requirement for organizations to provide a notice of a breach of security of personal data or other company information. However, in certain cases provided for by the Federal Law on Personal Data of July 27, 2006, as amended, organizations that are personal data operators (companies that independently or jointly with other companies arrange for and/or perform personal data processing as well as determine purposes for personal data processing, categories of personal data subject to processing, actions/operations to be performed with personal data) must notify data subjects/their representatives and/or the Russian Federal Service for Supervision in the Sphere of Communications, Informational Technologies and Mass Communications (“Roskomnadzor”) of either eliminating a breach of personal data processing or destroying affected personal data.

The procedure is as follows:

1. Where allegations of illegal processing of personal data and/or processing of inaccurate personal data are made at the application/request by a data subject or his/her representative or the Roskomnadzor, a data operator must block illegally processed/inaccurate data or arrange for the blocking of said data (if the data processing is performed by a third party at the instruction of the operator) from the date of receipt of said application/request and during the entire period of inspection. In cases of processing of inaccurate personal data, blocking may be performed if it does not breach the rights and the legal interests of the data subject or third parties.

2. If, during the inspection, the allegation that personal data is inaccurate is confirmed, the operator must amend (arrange for amending) the data based on the information provided by the data subject, his/her representative, the Roskomnadzor or based on other documents, within 7 business days after provision of said information/documents. Personal data must then be unblocked upon correction.

3. If it is established that personal data has been processed illegally, a personal data operator must terminate illegal processing of personal data or arrange for such termination within 3 business days upon discovery of the violation. In case processing of personal data cannot be done in due course, the operator must destroy such personal data or arrange for its destruction within 10 business days upon discovery of the violation.

4. The personal data operator must notify the data subject or his/her representative and the Roskomnadzor (if the allegation that the data is processed illegally was made by the Roskomnadzor) of either elimination of
the breach or the destruction of personal data. There is no express timing for notification.

2. For each law and regulation identified in Question 1, please describe:

a. **The general scope of the breach notice requirement.**
The notice shall indicate whether the breach was cured or personal data was destroyed.

b. **The definition or standard of a covered “data breach.”**
Not specifically defined, but generally referenced as “illegal” actions regarding the processing of data.

c. **Whether it is mandatory to notify affected individuals.**
Yes.

d. **Whether it is mandatory to notify any government authorities.**
Yes, but only when the request of illegal processing of personal data was made by the Roskomnadzor.

e. **Whether any other parties may need to be notified of the incident.**
If the request of illegal processing of personal data was made by a representative of the data subject, such representative must also be notified of either the elimination of the breach or of the fact that personal data has already been destroyed.

f. **Whether the above rules are different if the company is acting as a data processor/service provider, and not acting as the data controller/owner of the information at issue.**
No.

g. **What are the potential penalties for non-compliance with the breach notice obligation?**
The potential penalties include a warning, an administrative fine, or civil actions.
Saudi Arabia

George Sayen
Riyadh
Tel: + 966 11 265 8900, Ext. 8911
george.sayen@bakermckenzie.com

Aisha Gondal
Riyadh
Tel: + 966 11 265 8900, Ext. 8913
aisha.gondal@bakermckenzie.com

Haifa Bahaian
Riyadh
Tel: + 966 11 265 8900, Ext. 8968
haifa.bahaian@bakermckenzie.com

Judes Abboud
Dubai
Tel: + 971 442 30080
judes.abboud@bakermckenzie.com
1. In your jurisdiction, are there legal requirements for organizations to provide notice of a breach of security for personal data or other company information?

In general, Saudi Arabia does not currently have any data breach notification law in effect nor does it have a national data protection authority. This means that personal data security breaches are not notified to any individual or entity in Saudi Arabia. However, a number of Saudi regulations impose a variety of penalties on breaching the privacy of confidential data, including amongst others, the Banking Control Law, the Telecommunications Law and Regulations and the Anti-Cyber Crime Law.

2. For each law and regulation identified in Question 1, please describe:

a. The general scope of the breach notice requirement.
   Not applicable.

b. The definition or standard of a covered “data breach.”
   Not applicable.

c. Whether it is mandatory to notify affected individuals.
   No.

d. Whether it is mandatory to notify any government authorities.
   No.

e. Whether any other parties may need to be notified of the incident.
   No.

f. Whether the above rules are different if the company is acting as a data processor/service provider, and not acting as the data controller/owner of the information at issue.
   No.

g. What are the potential penalties for non-compliance with the breach notice obligation?
   Not applicable.
Singapore

Ken Chia
Singapore
Tel: +65 6434 2558
ken.chia@bakermckenzie.com
1. In your jurisdiction, are there legal requirements for organizations to provide notice of a breach of security for personal data or other company information?

Yes.

Please identify the name of the relevant law(s) or regulation(s).

The Monetary Authority of Singapore Notices on Technology Risk Management (“TRM Notices”).

Please note that the Personal Data Protection Act 2012, which governs the use, collection and disclosure of personal data, does not currently require that an organization provide a notice of breach of security for personal data.

2. For each law and regulation identified in Question 1, please describe:

a. The general scope of the breach notice requirement.

The TRM Notices require “financial institutions” to notify the Monetary Authority of Singapore (“MAS”) as soon as possible, but not later than 1 hour, from the discovery of a “relevant incident”.

“Financial institutions” include:

(1) All -

(a) approved exchanges;
(b) designated clearing houses;
(c) holders of a capital markets services license;
(d) recognized market operators which are incorporated in Singapore; and
(e) persons who are approved under section 289 of the Securities and Futures Act to act as a trustee of a collective investment scheme which is authorized under section 286 of the Securities and Futures Act and constituted as a unit trust.

(2) All licensed financial advisers;
(3) All licensed insurers, other than captive insurers and marine mutual insurers;
(4) All registered insurance brokers;
(5) All banks in Singapore;
(6) All credit card or charge card licensees in Singapore;
(7) All finance companies;
(8) All money brokers approved under section 28 of the Monetary Authority of Singapore Act;
(9) All merchant banks approved under section 28 of the Monetary Authority of Singapore Act;
(10) All holders of a remittance license issued under section 8 of the Money-changing and Remittance Businesses Act;
(11) All operators and settlement institutions of designated payment systems; and
(12) All trust companies licensed under the Trust Companies Act

“Relevant incident” is defined as a system malfunction or IT security incident, which has a severe and widespread impact on the [financial institution’s] operations or materially impacts the [relevant financial institution’s] service to its customers.”

We believe that the breach of security for personal data or company information could potentially amount to or contribute to a “relevant incident,” and thus the notification requirements as described above could potentially apply in such circumstance.

b. The definition or standard of a covered “data breach.”

Please see above definition of “relevant incident.”

c. Whether it is mandatory to notify affected individuals.

No.

d. Whether it is mandatory to notify any government authorities.

Yes.

The TRM Notices require financial institutions to notify the Monetary Authority of Singapore (“MAS”) as soon as possible, but not later than 1 hour, from the discovery of a “relevant incident.”

e. Whether any other parties may need to be notified of the incident.

No.

f. Whether the above rules are different if the company is acting as a data processor/service provider, and not acting as the data controller/owner of the information at issue.

No.

g. What are the potential penalties for non-compliance with the breach notice obligation?

Penalties will vary based on the type of financial institution which is found to be in non-compliance with the breach notification obligation described above. Maximum fines range from $20,000 - $150,000 per offence, and further
maximum fines of between $2,000 - $15,000 per day for continuing offences. For some financial institutions, directors and managers may also be found liable for non-compliance with the breach notice obligations.
South Africa

Darryl Bernstein
Johannesburg
Tel: +27 (0) 11 911 4367
darryl.bernstein@bakermckenzie.com

Widaad Ebrahim
Johannesburg
Tel: +27 (0) 11 911 4384
widaad.ebrahim@bakermckenzie.com

Deepa Ramjee
Johannesburg
Tel: +27 (0) 11 911 4368
deepa.ramjee@bakermckenzie.com
1. In your jurisdiction, are there legal requirements for organizations to provide notice of a breach of security for personal data or other company information?

No.

While South African law does not presently require or impose notification obligations to be adopted, in the event of a security breach of personal data (of individuals and juristic persons), the Protection of Personal Information Act, 2013 (POPI), once fully commenced, will indeed require organisations to provide notice of a breach of security. To date, only certain sections of POPI have commenced, particularly, those dealing with the establishment of the Information Regulator and its powers to draft and put forward regulations under POPI. Consequently, the bulk of POPI has yet to commence and significantly, compliance is not yet enforceable.

2. For each law and regulation identified in Question 1, please describe:

a. The general scope of the breach notice requirement.

The scope of the breach notice requirement under POPI is quite broad and applies to any type of “personal information,” defined as any information relating to an identifiable, living, natural person, and where applicable, an identifiable, existing juristic person, including, but not limited to:

(a) information relating to the race, gender, sex, pregnancy, marital status, national, ethnic or social origin, colour, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language and birth of the person;

(b) information relating to the education or the medical, financial, criminal or employment history of the person;

(c) any identifying number, symbol, e-mail address, physical address, telephone number, location information, online identifier or other particular assignment to the person;

(d) the biometric information of the person;

(e) the personal opinions, views or preferences of the person;

(f) correspondence sent by the person that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence;

(g) the views or opinions of another individual about the person; and
(h) the name of the person if it appears with other personal information relating to the person or if the disclosure of the name itself would reveal information about the person.

This broad classification of personal information is not limited to type / industry.

b. The definition or standard of a covered “data breach.”

Mindful that the operative provisions of POPI have yet to commence, there is no guidance on a particular definition or standard of a covered “data breach.”

A responsible party must secure the integrity and confidentiality of personal information in its possession or under its control by taking appropriate and reasonable technical and organizational measures to prevent: loss of, damage to or unauthorized destruction of personal information; and unlawful access to or processing of personal information.

Where there are reasonable grounds to believe that the personal information of a data subject has been accessed or acquired by any unauthorised person, the breach notice requirements under POPI kick in. POPI does not, currently, contemplate any exceptions to the above notification requirement.

c. Whether it is mandatory to notify affected individuals.

Yes.

If the identity of the data subject can be established, the notification to the data subject must be made as soon as reasonably possible after the discovery of the compromise, taking into account the legitimate needs of law enforcement or any measures reasonably necessary to determine the scope of the compromise and to restore the integrity of the responsible party’s information system. The responsible party may only delay notification of the data subject if a public body responsible for the prevention, detection or investigation of offences or the Information Regulator determines that notification will impede a criminal investigation by the public body concerned.

The notification to a data subject must be in writing and communicated to the data subject in at least one of the following ways:

(a) emailed to the data subject’s last known physical or postal address;
(b) sent by e-mail to the data subject’s last known e-mail address;
(c) placed in a prominent position on the website of the responsible party;
(d) published in the news media; or
(e) as may be directed by the Regulator.
The notification must provide sufficient information to allow the data subject to take protective measures against the potential consequences of the compromise, including:

(a) a description of the possible consequences of the security compromise;

(b) a description of the measures that the responsible party intends to take or has taken to address the security compromise;

(c) a recommendation with regard to the measures to be taken by the data subject to mitigate the possible adverse effects of the security compromise; and

(d) if known to the responsible party, the identity of the unauthorised person who may have accessed or acquired the personal information.

d. **Whether it is mandatory to notify any government authorities.**

Yes.

The notification to the Information Regulator must be made as soon as reasonably possible after the discovery of the compromise, taking into account the legitimate needs of law enforcement or any measures reasonably necessary to determine the scope of the compromise and to restore the integrity of the responsible party’s information system. The content of this notification will likely be the same as the notice to the data subject, namely:

(a) a description of the possible consequences of the security compromise;

(b) a description of the measures that the responsible party intends to take or has taken to address the security compromise;

(c) a recommendation with regard to the measures to be taken by the data subject to mitigate the possible adverse effects of the security compromise; and

(d) if known to the responsible party, the identity of the unauthorised person who may have accessed or acquired the personal information.

e. **Whether any other parties may need to be notified of the incident.**

Yes.

The Information Regulator may direct a responsible party to publicise, in any manner specified, the fact of any compromise to the integrity or confidentiality of personal information, if the Regulator has reasonable grounds to believe that such publicity would protect a data subject who may be affected by the compromise. In these circumstances, the timing and content of the notification would likely be clarified by the Information Regulator on a case by case basis.
f. Whether the above rules are different if the company is acting as a data processor/service provider, and not acting as the data controller/owner of the information at issue.

Yes.

Under POPI while a responsible party/data controller must notify the Regulator and the data subject of a security compromise, an operator/data processor is only required to notify the responsible party.

The operator/data processor must notify the responsible party/data controller immediately where there are reasonable grounds to believe that the personal information of a data subject has been accessed or acquired by any unauthorised person.

There are no other requirements in relation to timing and content of the notification by a operator / data processor, save to say that the responsible party must have due regard to generally accepted information security practices and procedures, such procedures yet to be determined by the Information Regulator.

g. What are the potential penalties for non-compliance with the breach notice obligation?

Depending on the breach or offence, potential penalties for non-compliance include administrative fines (not exceeding ZAR10 million), penalties (a fine or imprisonment for a period not exceeding 10 years or both a fine and such imprisonment) or sanctions, or civil actions and/or class actions.
South Korea

Boseong Kim
Seoul
Tel: +82 2 721 4130
boskim@kcllaw.com

Junghwa Lee
Seoul Tel: +82 2 721 4147
jhlee@kcllaw.com
1. In your jurisdiction, are there legal requirements for organizations to provide notice of a breach of security for personal data or other company information?

Yes.

**Please identify the name of the relevant law(s) or regulation(s).**

- Personal Information Protection Act (PIPA);
- Act on Promotion of Information Communications Network Utilization and Information Protection (Information Communications Network Act).

2. For each law and regulation identified in Question 1, please describe:

a. **The general scope of the breach notice requirement.**

Under PIPA, the relevant breach notice requirement may apply to:

(i) any types of personal information, including without limitation sensitive information and credit information as it is applicable for any event of breach of personal information and

(ii) all industry sectors and all company types.

Under the Information Communications Network Act, the relevant breach notice requirement may apply to:

(i) any types of personal information of users, including without limitation sensitive information and credit information,

(ii) any information and communications service providers such as telecommunications companies and internet service providers and

(iii) the event of an attack to an information and communications network or information system by means of hacking or other means and the event of a loss, theft or leakage of personal information.

b. **The definition or standard of a covered “data breach.”**

Under PIPA: The guidelines on personal information protection adopted by the Ministry of Public Administration and Security defines a data breach as a loss of control by the personal information processor over, or an authorized access to, personal information of data subjects, without basis on laws or regulations or the data subjects own will, which is one of the following events:

(1) loss or theft of a writing, portable storage device or portable computer, etc. that contains personal information;
(2) access by an authorized person to a personal information processing system such data base, etc. that contains personal information;

(3) delivery of a file, written document or other storage device that contains personal information to an unauthorized person due to a willful misconduct or negligence of the personal information processor;

(4) other delivery of personal information to an unauthorized person or access allowed to an unauthorized person to an personal information processing system.

Under the Information Communications Network Act:
The relevant breach notice requirement arises in the event of a loss, theft or leakage of personal information. For your information, an event of intrusion is defined under the Information and Communications Network Act as an event that occurs due to an attack to an information and communications network or an information system related to such a network by means of hacking, computer viruses, logic bombs, mail bombs, denial of service, high-power electromagnetic wave, etc. The service provider has no breach notification requirement in the event of an intrusion (e.g., hacking) under the Information Communications Network Act.

c. Whether it is mandatory to notify affected individuals.
Yes.

Under PIPA, the notification must be made without delay. The content of notification must include:

(i) categories of personal information that have been breached;
(ii) time of data breach and how the data breach has occurred;
(iii) information on the steps that may be taken by the data subjects to minimize potential damages from the data breach;
(iv) description of the steps taken by the personal information processor in response and relief for damages;
(v) contact information of the department that may be contacted by the data subjects to report damages.

Under the Information and Communications Network Act:
In the event of a leakage of personal information, the information and communications service provider must notify the affected individuals without delay (which means within 24 hours from when the service provider becomes aware that personal information has leaked out under normal circumstances).

The notification should include:
(i) categories of personal information that have leaked out;
(ii) time of leakage;
(iii) steps that may be taken by the data subjects in response;
(iv) description of the steps taken by the service provider in response;
(v) contact information of the department of the service provider that may be contacted by the data subjects for advice, etc.

For your information, the service provider would not be obligated to notify affected individuals in the event of an intrusion (e.g., hacking) under the Information Communications Network Act, but if the intrusion has caused a leakage of personal information, the service provider would be obligated to comply with the notification requirements noted above.

d. Whether it is mandatory to notify any government authorities.

Yes.

Under PIPA: In the event of a data breach for personal information of 10,000 individuals or more, the notification should be filed without delay with the Ministry of the Interior, National Information Society Agency or Korea Internet & Security Agency.

Under the Information and Communications Network Act: In the event of a leakage of personal information, the notification should be filed with the Korea Communications Commission or Korea Internet & Security Agency, regardless of the scale of the leakage. In the event of an intrusion (e.g., hacking), the service provider should file an immediate report with the Ministry of Science, ICT and Future Planning or Korean Internet & Security Agency. The Information and Communications Network Act does not provide for the content of notification, but the service provider would need to file a detailed report.

e. Whether any other parties may need to be notified of the incident.

No.

f. Whether the above rules are different if the company is acting as a data processor/service provider, and not acting as the data controller/owner of the information at issue.

Yes.

Under PIPA: The above rules would not be different.

Under the Information and Communications Network Act: The information and communications service provider (and not the person to whom data
processing is outsourced) would have the relevant breach notification requirement. It should be the information and communications service provider who should have the breach notification requirement. If the data breach has occurred in relation to outsourced work, the outsourcing service provider would also be liable.

**g. What are the potential penalties for non-compliance with the breach notice obligation?**

Under PIPA: Non-compliance with the breach notification requirements may result in an administrative fine of up to KRW 30 million (approximately US$26,000).

Under the Information and Communications Network Act: In the event of a data breach, if the information and communications service provider fails to comply with the breach notification requirements, the service provider may be subject to an administrative fine up to KRW 30 million (approximately US$26,000). In the event of an intrusion (e.g., hacking), if the service provider fails to report the incident, etc., the service provider may be subject to an administrative fine up to KRW 10 million (approximately US$8,600).
Spain

Raul Rubio
Madrid
Tel: +34 91 436 6639
raul.rubio@bakermckenzie.com

Jordi Masdevall
Barcelona
Tel: +34 93 206 0820
jordi.masdevall@bakermckenzie.com

Rosario Alvarez
Madrid
Tel: +34 91 230 4513
rosario.alvarez@bakermckenzie.com
1. In your jurisdiction, are there legal requirements for organizations to provide notice of a breach of security for personal data or other company information?

Yes.

**Please identify the name of the relevant law(s) or regulation(s).**


2. For each law and regulation identified in Question 1, please describe:

   **a. The general scope of the breach notice requirement.**

   The breach notice requirement currently applies to a particular company-type only: providers of publicly available electronic communications services.

   The information included in this survey refers to the aforementioned type of company, as the legal obligation only applies to them.

   However, depending on the specific circumstances of the case, other companies may need to assess whether it is also appropriate for them to notify any entity/individual. For example, the company may have contractually assumed the obligation to notify (note that statements used in advertising may be considered binding vis-à-vis the user). In other cases, the breach may affect data such as credit card information. Notification to individuals (e.g., for them to cancel their credit card) may then be used as an argument to defend that the company acted with due diligence and claim that any possible sanction would need to be lower as a consequence of this diligent action. It may also be used to argue that any possible liability in case of fraud by means of the credit card information needs to be excluded/limited (otherwise, users may claim that the company knew that they could be subject to fraud and did not inform them). In any event, the benefits and down sides of a voluntary notification will need to be carefully analyzed by the company.

   Please also see information included in section 2(e) below on data processors.

   **b. The definition or standard of a covered “data breach.”**

   “Personal data breach” means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed in connection with the provision of a publicly available electronic communications service.
c. **Whether it is mandatory to notify affected individuals.**

Yes.

1. In the event of a particular risk of data breach concerning the public network or the electronic communications service, the subscribers must be notified without undue delay after the detection of the particular risk. Notification must inform of the existence of a material risk of breach and of the measures to be taken.

2. As a general rule, in the event of a data breach that is likely to adversely affect the personal data or privacy of a subscriber or individual, notification to such subscriber or individual must be sent without undue delay (and in any event it should be made within 24 hours after detection of the breach). This notification is not required if the operator has proven to the satisfaction of the Spanish Data Protection Authority that the appropriate measures have been taken with regard to the data affected by the breach. Such technological protection measures shall render the data unintelligible to any person who is not authorized to access it.

Content of the notification to the subscriber or individual:

1. Name of the provider
2. Identity and contact details of the data protection officer or other contact point where more information can be obtained
3. Summary of the incident that caused the personal data breach
4. Estimated date of the incident
5. Nature and content of the personal data concerned
6. Likely consequences of the personal data breach for the subscriber or individual concerned
7. Circumstances of the personal data breach
8. Measures taken by the provider to address the personal data breach
9. Measures recommended by the provider to mitigate possible adverse effects.

**d. Whether it is mandatory to notify any government authorities.**

Yes.

The Spanish Data Protection Agency is the recipient of the data breach notifications. Notification must be made through the electronic means provided by the Spanish Data Protection Agency on its website.
Notifications must be sent within 24 hours after the breach detection. The content of the notification is as follows:

**Section 1**

Identification of the provider

1. **Name of the provider**
2. **Identity and contact details of the data protection officer or other contact point where more information can be obtained**
3. **Whether it concerns a first or second notification**

Initial information on the personal data breach (for completion in later notifications, where applicable)

1. **Date and time of incident (if known; where necessary an estimate can be made), and of detection of incident**
2. **Circumstances of the personal data breach (e.g., loss, theft, copying)**
3. **Nature and content of the personal data concerned**
4. **Technical and organizational measures applied (or to be applied) by the provider to the affected personal data**
5. **Relevant use of other providers (where applicable)**

**Section 2**

Further information on the personal data breach

1. **Summary of the incident that caused the personal data breach (including the physical location of the breach and the storage media involved):**
2. **Number of subscribers or individuals concerned**
3. **Potential consequences and potential adverse effects on subscribers or individuals**
4. **Technical and organizational measures taken by the provider to mitigate potential adverse effects**

Possible additional notification to subscribers or individuals

1. **Content of notification**
2. **Means of communication used**
3. **Number of subscribers or individuals notified**
Possible cross-border issues

1. **Personal data breach involving subscribers or individuals in other Member States**

2. **Notification of other competent national authorities**

Where all the information set out above is not available and further investigation of the personal data breach is required, it is possible to make two separate notifications, as follows:

(i) an initial notification to the Spanish Data Protection Agency no later than 24 hours after the detection of the personal data breach. This initial notification shall include the information set out in section 1 above.

(ii) a second notification to the Spanish Data Protection Agency as soon as possible, and at the latest within 3 days following the initial notification. This second notification shall include the information set out in section 2 above and, where necessary, update the information already provided.

e. **Whether any other parties may need to be notified of the incident.**

Yes.

Even if the provider of publicly available electronic communications services only renders a part of the electronic communications service without having a direct contractual relationship with subscribers, it shall immediately inform the contracting provider in the case of a personal data breach.

Additionally, and following general data protection principles, data processors should inform the owner of the information at issue (data controllers) whenever there is a data breach.

In any event, please note that the assessment about whether any additional parties must be notified of the incident should be made taking into consideration the specific circumstances of the case and any possible contractual obligations that the company may have.

f. **Whether the above rules are different if the company is acting as a data processor/service provider, and not acting as the data controller/owner of the information at issue.**

No.

As a general rule, no. Please see specific reference to data processor in the previous question.
g. What are the potential penalties for non-compliance with the breach notice obligation?

Generally, failure to provide a notification when it is required under the General Telecommunications Act may be deemed a serious infringement with fines of up to EUR 2 million on the relevant company, and fines of up to EUR 30,000 on the legal representatives or members of the executive board involved in the decision or resolution. Fines could even surpass the aforementioned amount or include other complementary sanctions if the infringement is repeated.

Also note that the application of other sanctions arising from the personal data disclosure or other data protection infringements cannot be ruled out.
1. In your jurisdiction, are there legal requirements for organizations to provide notice of a breach of security for personal data or other company information?

Yes.

Please identify the name of the relevant law(s) or regulation(s).

- Electronic Communications Act (Sw. Lagen om elektronisk kommunikation) (“ECA”)
- Personal Data Act (Sw. Personuppgiftslagen) (“PDA”)

2. For each law and regulation identified in Question 1, please describe:

a. The general scope of the breach notice requirement.

   **Personal Data Act**

   The PDA is unclear regarding data breach notifications as there are no explicit provisions regarding data breach notifications. There is no official guidance available from the Swedish Data Inspection Board (Sw. Datainspektionen). Although there is no explicit provision on data breach notifications, a data controller may want to notify the affected data subjects in order to allow the data subjects to take mitigating actions thereby reducing the amount of damage suffered by data subjects. As there are no provisions regarding data breach notifications in the PDA, the answers to questions 2(b) to 2(g) below will only cover the data breach notification requirements of the ECA.

   **Electronic Communications Act**

   The data breach notification requirement applies to providers of publicly available electronic communication services, e.g., Internet service providers and telecom companies. The breach notification does not only apply to personal data but to all data processed in connection with the supply of publicly available electronic communication services.

b. The definition or standard of a covered “data breach.”

   Under the ECA, the term integrity incident (Sw. integritetsincident) is used and is defined as:

   “an event which leads to an unintentional or prohibited deletion, loss or change, or a prohibited disclosure of or prohibited access to information which is processed in connection with the supply of publicly available electronic communication services”.


The general rule under the Electronic Communications Act and Regulation EU 611/2013 is that all data breaches shall be notified to the Swedish Post and Telecom Authority (Sw. Post- och telestyrelsen) (“PTA”) and affected subscribers or users. Affected subscribers or users do not have to be notified if (i) the data breach cannot be assumed to have any adverse effect on the subscribers or users, or (ii) the service provider has taken technical safety measures which render the information affected by the data breach unintelligible for unauthorized persons, e.g., through encryption or hash function.

c. **Whether it is mandatory to notify affected individuals.**

It is mandatory to notify affected individuals if (i) the data breach can be assumed to have any adverse effect on the affected individuals, or (ii) if the PTA requests that notice shall be given to affected individuals. Affected individuals shall be notified “without undue delay” after the detection of the data breach. The assessment of what constitutes undue delay is decided in each individual case taking into account the individuals’ interest in and ability to take mitigating actions.

The notification shall contain the following information:

1. Name of the service provider
2. Identity and contact details of the data protection officer or other contact point where information can be obtained
3. Summary of the incident that caused the breach
4. Estimated date of the incident
5. Nature and content of the personal data concerned
6. Likely consequences of the data breach for the subscriber or individual concerned
7. Circumstances of the data breach
8. Measures taken by the service provider to address the data breach
9. Measures recommended by the service provider to mitigate possible adverse effects

d. **Whether it is mandatory to notify any government authorities.**

Yes.

An initial data breach notification must be provided to the PTA within 24 hours after the detection of the data breach (containing the information in 1-8 below). If all required information (1-17 below) is not available and further
investigation is required, a second notification must be provided within 72 hours of the initial notification.

The initial notification shall contain the following information:

1. Name of the service provider
2. Identity and contact details of the data protection officer or other contact point where more information can be obtained
3. Whether it concerns a first or second notification
4. Date and time of the incident (if known; where necessary an estimate can be made), and of detection of incident
5. Circumstances of the data breach (e.g. loss, theft, copying)
6. Nature and content of the personal data concerned
7. Technical and organizational measures applied (or to be applied) by the provider to the affected personal data
8. Relevant use of other providers (where applicable)
9. Summary of the incident that caused the personal data breach (including the physical location of the breach and the storage media involved)
10. Number of subscribers or individuals concerned
11. Potential consequences and potential adverse effects on subscribers or individuals
12. Technical and organisational measures taken by the provider to mitigate potential adverse effects
13. Content of notification to subscribers or individuals
14. Means of communication used
15. Number of subscribers or individuals notified
16. Data breach involving subscribers or individuals in other Member States
17. Notification of other competent national authorities

e. **Whether any other parties may need to be notified of the incident.**

No.
f. Whether the above rules are different if the company is acting as a data processor/service provider, and not acting as the data controller/owner of the information at issue.

No.

g. What are the potential penalties for non-compliance with the breach notice obligation?

The PTA may issue injunctive orders. Such orders may be combined with a conditional fine (based on the financial standing of the company) to be paid in case of non-compliance with the injunctive order. However, according to the information available on the PTA’s website there have been no cases where the PTA has issued an injunctive order for failure to comply with data breach notification obligations.

If a data breach is caused by a service provider’s failure to implement appropriate technical and organizational safety measures to protect personal data, the service provider may be liable to pay damages to affected individuals. Failure to notify an affected individual of a breach may increase the amount of damage or violation of privacy suffered by an individual and consequently increase the liability of the service provider.
Switzerland

Nicolas Passadelis
Zurich
Tel: +41 44 384 1209
nicolas.passadelis@bakermckenzie.com
1. In your jurisdiction, are there legal requirements for organizations to provide notice of a breach of security for personal data or other company information?

No.

2. For each law and regulation identified in Question 1, please describe:

a. **The general scope of the breach notice requirement.**

Neither the Swiss Data Protection Act (DPA) nor other laws explicitly deal with security breaches. Therefore, there are no statutory requirements or established practices for notifying the data subjects or authorities in case of a security breach. However, one may argue that the obligation to notify comes from the general obligation to process data in good faith or the obligation to mitigate any damages potentially incurred by the data subject. Notification may also be contractually required if there is an agreement between the data controller and the data subject explicitly or implicitly imposing a notification obligation on the relevant organization. Concerned organizations must, therefore, decide on a case-by-case basis whether to notify in the event of a security breach. Despite the absence of a mandatory data breach notification obligation, we recommend notification of data breaches to avoid negative publicity for the affected organizations.

The details of the notification must be determined on a case-by-case basis. Notifying the data subjects directly seems more preferable than publishing the notification in newspapers and other media. The notification should include, at a minimum:

(i) information on the date of disclosure;

(ii) identity of the data controller;

(iii) data subjects affected;

(iv) the data categories affected;

(v) the circumstances of disclosure;

(vi) possible risks for the data subjects;

(vii) security measures taken by the data controller to mitigate the damage and prevent further disclosure;

(viii) a contact person for the data subjects.
b. The definition or standard of a covered “data breach.”

As Swiss laws do not explicitly deal with security breaches, there is no statutory definition of a data security breach. Due to the lack of case law and any official guidance by the Federal Data Protection and Information Commissioner (the Data Protection Commissioner) dealing with data security breaches, there is also no generally accepted definition of a data security breach.

In accordance with the DPA, we would define a data security breach as an unintentional disclosure of personal data due to the existence or failure of technical and organizational security measures. According to this definition, the simple unauthorized access of information as well as any unauthorized access and further use of personal data will be qualified as data security breach.

c. Whether it is mandatory to notify affected individuals.

No.

d. Whether it is mandatory to notify any government authorities.

No.

e. Whether any other parties may need to be notified of the incident.

No.

f. Whether the above rules are different if the company is acting as a data processor/service provider, and not acting as the data controller/owner of the information at issue.

Yes.

The potential data breach notification requirements described above, in principle, apply to data controllers. In exceptional cases, data processors may also be subject to the relevant requirements, e.g., in the event the data controller is unable to notify the data breach.

g. What are the potential penalties for non-compliance with the breach notice obligation?

Although there are no statutory foreseen penalties for security breaches, the impact of a security breach that becomes public can be manifold: A security breach that affects a major number of data subjects can trigger an investigation by the Data Protection Commissioner. While the Data Protection Commissioner cannot impose any sanctions on the relevant organization or its directors and officers, he can issue recommendations that must be complied with. If the security breach concerns information that is subject to confidentiality obligations stemming from other laws such as administrative
laws (e.g., for financial institutions or insurance companies) or criminal laws, public prosecutors or regulatory may also initiate investigations. Such investigations may entail publicity and, therefore, cause reputational harm.

Violating data protection obligations may also result in civil liability. The data subject may sue the organization for correction, cease and desist, deletion and damages covering financial losses or lost profits incurred by the data subject.

Security breaches do not, in principle, lead to fines under Swiss law even if the security breaches are due to insufficient organizational or technical security measures. Only certain violations of a data protection obligation by private persons are subject to penal sanctions and a fine:

(i) failing intentionally to comply with access rights or information obligations;

(ii) failing intentionally to register accurately their data collections or to notify the Federal Data Protection and Information Commissioner on the safeguards implemented for the cross-border transfer of personal data to countries that do not provide an adequate level of protection;

(iii) failing intentionally to cooperate in investigations by the Commissioner or providing inaccurate information;

(iv) disclosing intentionally and without authorization confidential and particularly sensitive information or personality profiles obtained in a professional function that requires the knowledge of such data or while working for a third party subject to confidentiality obligations.
Taiwan

H. Henry Chang
Taipei
Tel: +886 2 2715 7259
henry.chang@bakermckenzie.com

Chris Tsai
Taipei
Tel: +886 2 2715 7310
chris.tsai@bakermckenzie.com
1. In your jurisdiction, are there legal requirements for organizations to provide notice of a breach of security for personal data or other company information?

Yes.

Please identify the name of the relevant law(s) or regulation(s).

- Personal Data Protection Act ("PDPA")

2. For each law and regulation identified in Question 1, please describe:

a. The general scope of the breach notice requirement.
   The law covers all data collectors who violate the PDPA requirements and thus cause the personal data to be stolen, disclosed, altered, or infringed in other ways.

b. The definition or standard of a covered “data breach.”
   Notification is not required if the incident is not due to violations of the PDPA.

c. Whether it is mandatory to notify affected individuals.
   Yes.
   Notification should be made immediately after the data collector makes its own inspection. The content of the notification shall include the fact that personal data has been infringed and the corresponding measures which have been undertaken.

d. Whether it is mandatory to notify any government authorities.
   No.

e. Whether any other parties may need to be notified of the incident.
   No.

f. Whether the above rules are different if the company is acting as a data processor/service provider, and not acting as the data controller/owner of the information at issue.
   No.

g. What are the potential penalties for non-compliance with the breach notice obligation?
   The competent authorities shall order the data collector to rectify the violation within a given period. If the violation is not rectified within the given period, an
administrative fine of NT$20,000 to NT$200,000 shall be imposed each time such violation occurs. The legal representative, manager, or other representative of such violating data collector who should be subject to an administrative fine due to the violation of the PDPA should be subject to the same amount of the fine, unless the obligation of the representative has been proved to be fulfilled.
Thailand

Dhiraphol Suwanprateep
Bangkok
Tel: +66 02 636 2000 Ext. 4950
dhiraphol.suwanprateep@bakermckenzie.com

Pattaraphan Paiboon
Bangkok
Tel: +66 02 636 2000 Ext. 4568
pattaraphan.paiboon@bakermckenzie.com
1. In your jurisdiction, are there legal requirements for organizations to provide notice of a breach of security for personal data or other company information?

Yes, however, the legal requirements vary depending on the industries involved. The relevant laws and regulations in each industry are as follows:

- Notification of the National Telecommunications Commission Re: Measures for Protection of Telecommunications Service Users’ Rights Related to Personal Information, Privacy Rights and Freedom to Communicate by Means of Telecommunications (the “Privacy Notification”);
- A Guideline on the Security of Credit Information Services (“The Guideline”); and
- The Personal Data Protection Bill, currently not issued but expected to be passed within this year (“The Personal Data Protection Bill”).

2. For each law and regulation identified in Question 1, please describe:

a. The general scope of the breach notice requirement.

Currently, Thailand does not have a consolidated data privacy law in general. However, the Personal Data Protection Bill is under consideration.

For specific sectors, there are data privacy restrictions under specific laws e.g., telecommunications business, credit information and the Personal Data Protection Bill.

(1) Mandatory Breach Notification

- The Telecommunications Business Act and the Privacy Notification

  If there is a breach of the telecommunications users’ rights in relation to personal information, privacy, or the right to communicate through telecommunications, telecommunications operators must notify affected users without delay.

- The Personal Data Protection Bill

  If the Personal Data Protection Bill is passed in its current form, there will be a requirement for breach notification. The personal data controller is
required to notify the data owner of the breach and the cause of breach immediately, and also the remedial plan for damage caused by such breach. If the breach affects greater than a number of people to be prescribed by the Data Protection Committee, the personal data controller must also report the breach to the Data Protection Committee.

(2) Other Requirements on Data Security Breach

According to the Credit Bureau Act and the Guideline, a credit bureau company for which the data security has been breached must promptly communicate, clarify, and create an understanding with staff, media, members and users of the problem and the proposed solution.

Furthermore, a report made in writing on the security breach must be provided to the board of directors of the credit bureau company.

b. The definition or standard of a covered “data breach.”

Please see our response in item 2(a).

In addition, according to the Personal Data Protection Bill, a person acting on another person or juristic person’s order e.g., employees, contractors, or online data collection service providers are not considered data controllers. Thus, such person does not have to comply with the Personal Data Protection Bill’s data breach notification obligations.

c. Whether it is mandatory to notify affected individuals.

Yes.

For timing of the notification, the relevant laws and regulations only prescribe that the notification shall be done without delay, promptly, or immediately as shown in section 2(a) without prescribing any specific period.

Telecommunications Business Act requires the license holders to notify the breach and the remedy. As for the Personal Data Protection Bill, the data controller must notify the cause of the breach and the remedial plan for damage caused by such breach.

d. Whether it is mandatory to notify any government authorities.

No.

e. Whether any other parties may need to be notified of the incident.

Yes.

According to the Guideline, the credit bureau company may need to communicate, clarify, create an understanding with third parties as described in section 2(a).
The Telecommunications Business Act or the Personal Data Protection Bill does not require notifying third parties apart from notifying affected users or the data owner or the Data Protection Committee as described in 2(a).

f. **Whether the above rules are different if the company is acting as a data processor/service provider, and not acting as the data controller/owner of the information at issue.**

Yes.

Under the Personal Data Protection Bill, the person acting on another person or juristic person’s order e.g., employees, contractors, or online data collection service providers are not considered data controllers. Thus, the above rule is different as such person does not have to comply with the Personal Data Protection Bill’s data breach notification obligations.

However, the above rules are not different for the Telecommunications Business Act and the Guideline as they govern telecommunications license business holder and credit bureau company, respectively.

g. **What are the potential penalties for non-compliance with the breach notice obligation?**

According to the Telecommunications Business Act, if the licensee violates or fails to comply with the breach notice obligation, the licensee may be subject to an administrative order, administrative fine, suspension or revocation of license.

Under the Personal Data Protection Bill, the data controller who fails to comply with the breach notice obligation could be subject to fines and/or imprisonment.
Turkey

Hakki Can Yildiz
Istanbul
Tel: +90 212 376 64 54
can.yildiz@esin.av.tr

Can Sozer
Istanbul
Tel: +90 212 376 64 43
can.sozer@esin.av.tr
1. In your jurisdiction, are there legal requirements for organizations to provide notice of a breach of security for personal data or other company information?

Yes.

Please identify the name of the relevant law(s) or regulation(s).

Law No. 6698 on Protection of Personal Data (the “Data Protection Law”) which entered into force on April 7, 2016. Secondary regulations based on the Data Protection Law will be issued until April 7, 2017.

2. For each law and regulation identified in Question 1, please describe:

a. The general scope of the breach notice requirement.

   Under the Data Protection Law, the breach notice requirement applies to all kinds of personal data. Secondary regulations are expected to bring further details.

b. The definition or standard of a covered “data breach.”

   The Data Protection Law does not provide any definition for “data breach” or any exceptions to the breach notice requirement. Secondary regulations are expected to bring further details.

c. Whether it is mandatory to notify affected individuals.

   Yes.

   Under Article 12/5 of the Data Protection Law, the breach notice must be made to the affected individuals within the shortest time possible. The mandatory content of the notification is not regulated in the Data Protection Law. Secondary regulations are expected to bring further details.

d. Whether it is mandatory to notify any government authorities.

   Yes.

   Under Article 12/5 of the Data Protection Law, the breach notice must be made to the Data Protection Authority, which is to be established by October 7, 2016, within the shortest time possible. The mandatory content of the notification is not regulated in the Data Protection Law. Secondary regulations are expected to bring further details.
e. Whether any other parties may need to be notified of the incident.

Yes.

Under Article 12/5 of the Data Protection Law, the Data Protection Authority may decide to announce the data breach on its own website or by another method it may deem appropriate. Secondary regulations are expected to bring further details.

f. Whether the above rules are different if the company is acting as a data processor/service provider, and not acting as the data controller/owner of the information at issue.

Yes.

Under Article 12/5 of the Data Protection Law, the data breach notice requirement applies to the data controller, not the data processor. Secondary regulations are expected to bring further details.

g. What are the potential penalties for non-compliance with the breach notice obligation?

Under Article 18/1(b) of the Data Protection Law, infringement of obligations in relation to data security (including data breach notice requirement) will result in an administrative fine of TRY 15,000 to 1,000,000. This article will enter into force on October 7, 2016.
Ukraine

Oleksiy Stolyarenko
Kyiv
Tel: +380 44 590 0101
oleksiy.stolyarenko@bakermckenzie.com
1. In your jurisdiction, are there legal requirements for organizations to provide notice of a breach of security for personal data or other company information?

Yes.

Please identify the name of the relevant law(s) or regulation(s).

- The Law Of Ukraine On Protection Of The Information In Information And Telecommunication Systems (Law)

2. For each law and regulation identified in Question 1, please describe:

a. The general scope of the breach notice requirement.

The breach notice requirement applies to all information, including:

(i) personal data,
(ii) commercial and trade secrets,
(iii) state secrets,
(iv) confidential information.

b. The definition or standard of a covered “data breach.”

Notification is required for any data breach and data breach attempt.

c. Whether it is mandatory to notify affected individuals.

No.

d. Whether it is mandatory to notify any government authorities.

Yes.

CERT-UA (abbr. - Computer Emergency Response Team of Ukraine - team that responds to computer emergencies in Ukraine) - a specialized structural unit of the State Center On Countering Cyber Threats at State Special Communications and Protection of Information Service of Ukraine. The law does not establish a standard for the timing or the content, but CERT-UA recommends the submission of information on the nature of a cyber threat, contact information and detailed description of the attack.

e. Whether any other parties may need to be notified of the incident.

No.
f. Whether the above rules are different if the company is acting as a data processor/service provider, and not acting as the data controller/owner of the information at issue.

No.

g. What are the potential penalties for non-compliance with the breach notice obligation?

The Law does not establish specific penalties or liability for non-compliance with the breach notice obligation.
United Kingdom

Robbie Downing
London
Tel: +44 20 7919 1161
robbie.downing@bakermckenzie.com

Dyann-Heward Mills
London
Tel: +44 20 7919 1269
dyann.heward-mills@bakermckenzie.com

Benjamin Slinn
London
Tel: +44 20 7919 1783
benjamin.slinn@bakermckenzie.com
1. In your jurisdiction, are there legal requirements for organizations to provide notice of a breach of security for personal data or other company information?

Yes.

Please identify the name of the relevant law(s) or regulation(s).

- Notification of data security breaches to the Information Commissioner’s Office ("ICO") Guidance ("Guidance")

2. For each law and regulation identified in Question 1, please describe:

a. The general scope of the breach notice requirement.

Under PECR and the Commission Regulation (EU) 611/2013, organisations providing public electronic communications services (e.g. telecoms providers and internet service providers) are required to notify the ICO within 24 hours of becoming aware of a personal data breach, along with information about the breach (where feasible). In addition, full details of the breach need to be provided to ICO within 3 days but where this is not possible, a justification for the delay must be provided to the ICO with full details to follow without undue delay.

Public electronic communications service providers are also required to notify affected individuals without undue delay if the breach is likely to adversely affect such individuals. If such a provider does not notify the relevant individuals as required, ICO may require the service provider to do so, having considered the likely adverse effects of the breach. Public electronic communications service providers are also required to maintain a log of any such breaches, which must be submitted to the ICO on a monthly basis.

Under the Data Protection Act 1998 (DPA), there is currently no general obligation on data controllers to notify either individual data subjects or ICO in the event of a security breach. However, ICO has issued Guidance which sets out the circumstances in which it expects serious data security breaches to be notified to ICO.

b. The definition or standard of a covered “data breach.”

The breach notification obligations under PECR apply to a “personal data breach”, which is defined as 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 public electronic communications service.

A “data breach” is not defined under the DPA. However, a data breach would generally cover the loss or misappropriation of personal data in breach of the obligation to take appropriate technical and organisational measures against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data. However, ICO in its Guidance states that it expects “serious” breaches to be reported to it (please see 2.d below).

c. Whether it is mandatory to notify affected individuals.
Yes.

Under PECR, public electronic communications service providers are required to notify affected individuals without undue delay if the personal data breach is likely to adversely affect such individuals. The notification to the individual must contain at least: (a) a description of the nature of the breach; (b) information about the contact points within the service provider’s organisation, from which more information can be obtained by the individual; and (c) recommendations for measures to allow the individual to mitigate the possible adverse impacts of the personal data breach.

The public electronic communications service provider is not required to notify the relevant individuals if it has demonstrated to ICO’s satisfaction that the service provider has implemented appropriate technological protection measures which render the data unintelligible to any person not authorised to access it and those measures were applied to the data concerned in that breach.

Although not mandatory under the DPA, ICO mentions in its Data Security Breach Management Guidance that providing information can be an important element in the organisation’s breach management strategy. Any notification to an affected individual should have a clear purpose, such as to enable the individual to take steps to protect him/herself. When notifying individuals, ICO recommends that specific and clear advice should be given on the steps the individual can take to protect him/herself and what the organisation is willing to do to help them.

d. Whether it is mandatory to notify any government authorities.
Yes.

It is mandatory for public electronic communications service providers to notify ICO in the event of a personal data breach. The initial notification must include: (a) the name of the service provider; (b) the name and contact details of the data protection officer or other contact point where more information can be obtained; (c) whether it is an initial notification or a full notification; (d)
the date and time of the breach (or an estimate) and the date and time of detection; (e) the circumstances of the breach; (f) the nature and content of the personal data concerned; (g) technical and organisational measures applied (or to be applied) to the affected personal data; and (h) relevant use of providers (where applicable). Additional information such as the number of individuals concerned, the potential consequences and adverse effects on individuals etc. should be provided in the initial notification or as soon as possible.

There is a secure PECR security breach notification web form on the ICO website for public electronic communications service providers to report breaches to ICO.

In relation to the DPA, ICO expects to be notified of “serious” data security breaches. “Serious breaches” are not defined, although the ICO does set out various factors that a data controller should consider to determine whether a breach is serious enough to be reported to ICO. These factors include the potential detriment to data subjects, the volume of personal data, and the sensitivity of the personal data. The greater the actual or potential detriment to the data subject, as a result of the volume and/or sensitivity of the data involved, the greater the presumption to report the breach to ICO. ICO has provided a data protection breach notification form to use when reporting a breach of the DPA to ICO. This form requires the following information to be provided: (a) organisation details (e.g. name, registration number etc); (b) details of the breach; (c) the personal data at risk; (d) steps taken regarding containment and recovery; (e) training and guidance provided to staff; (f) previous contact with ICO.

Under the Communications Act of 2003, public electronic communications network providers are required to notify OFCOM of a breach of security which has a significant impact on the operation of a public electronic communications network. In addition, public electronic communications service providers are required to notify OFCOM of a breach of security which has a significant impact on the operation of the relevant public electronic communications service. OFCOM may require the network or service provider to inform the public if OFCOM thinks it is in the public interest to do so. Major incidents or incidents which are likely to generate media or political interest should be reported within 24 hours. Other incidents should be reported within a few days of the incident, or in batches where there are a significant number of “non-major” incidents.
e. Whether any other parties may need to be notified of the incident.

Yes.

ICO mentions in its Data Security Breach Management Guidance that organisations may need to consider notifying third parties such as the police, insurers, professional bodies, bank or credit card companies that can assist in reducing the risks of financial loss to individuals, and trade unions. ICO will not normally tell the media or other third parties about a breach notified to ICO, but it may advise the data controller to do so.

f. Whether the above rules are different if the company is acting as a data processor/service provider, and not acting as the data controller/owner of the information at issue.

Yes.

The notification obligations under PECR apply to providers of public electronic communications services, which is any electronic communications service that is provided so as to be available for use by members of the public. An electronic communications service is any electrical, magnetic or electromagnetic signals (including speech, music, sounds, visual images or data of any kind) conveyed over an electronic communications network, other than a content service (e.g. a service providing material with a view to it being comprised of signals conveyed via an electronic communications network, or the exercise of editorial control over the contents of signals conveyed via such a network).

The obligations under the DPA, and ICO’s expectation in its guidance that serious data security breaches should be notified to it and in certain circumstances to data subjects, apply to data controllers (i.e. the entity that decides how and why personal data is processed) and not directly to data processors. However, data processors/service providers may be under contractual obligations to notify the data controller and other parties and to provide certain assistance in the event of a data security breach in the relevant contract between the data controller and the data processor/service provider.

g. What are the potential penalties for non-compliance with the breach notice obligation?

If a public electronic service provider fails to comply with the notification requirements under PECR, ICO can issue a fixed monetary penalty notice of £1,000. If the service provider pays £800 within 21 days of receiving the notice of intent from ICO, which includes amongst other information the date on which ICO proposes to serve a fixed monetary penalty notice, the service provider will avoid liability for the fixed monetary penalty.
There are no specific penalties for failure to comply with the notification obligations under the Guidance in relation to the DPA. However, ICO can impose fines of up to £500,000 for serious breaches of the DPA, which can include a serious breach of the obligation to take appropriate technical and organisational measures against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
United States

Amy de La Lama
Chicago
Tel: +1 312 861 2923
amy.delalama@bakermckenzie.com

Brian Hengesbaugh
Chicago
Tel: +1 312 861 3077
brian.hengesbaugh@bakermckenzie.com

Lothar Determann
Palo Alto
Tel: +1 650 856 5533
lothar.determann@bakermckenzie.com

Heather Mantegna
Chicago
Tel: +1 312 861 8808
heather.mantegna@bakermckenzie.com

Jeff Dunifon
New York
Tel: +1 212 626 4323
jeff.dunifon@bakermckenzie.com

Lindsay Martin
Chicago
Tel: +1 312 861 2949
lindsay.martin@bakermckenzie.com

Michael Egan
Washington, D.C.
Tel: +1 202 452 7022
michael.egan@bakermckenzie.com

Brandon Moseberry
Chicago
Tel: +1 312 861 8265
brandon.moseberry@bakermckenzie.com

Michael Stoker
Chicago
Tel: +1 312 861 2870
michael.stoker@bakermckenzie.com
1. In your jurisdiction, are there legal requirements for organizations to provide notice of a breach of security for personal data or other company information?

Yes.

**Please identify the name of the relevant law(s) or regulation(s).**

Federal and state laws establish mandatory duties to notify data breaches in the United States. At the federal level, key data breach notification obligations are established pursuant to:

- The Health Insurance Portability and Accountability Act, as amended by the Health Information Technology for Economic and Clinical Health Act ("HITECH") and the Genetic Information Nondiscrimination Act of 2008 ("GINA") (collectively, "HIPAA") (as implemented in 45 C.F.R. Parts 160, 162, and 164; and 42 USC §1320d, *et seq.*); and


In addition, the Federal Trade Commission ("FTC") actively pursues cases involving data breaches pursuant to its unfair or deceptive trade practices authority (15 U.S.C. §45, *et seq.*), among other powers.

At the state level, all but three states (New Mexico, Alabama, and South Dakota) establish breach notification duties:


For purposes of illustration, this US chapter summarizes certain aspects of breach notification requirements under HIPAA and GLBA, as well as the state data breach notification requirements in California, the District of Columbia, Florida, Illinois, Massachusetts, New York, and Texas. Note that an organization that experiences a data breach affecting US operations or individuals should not rely on summary analysis of applicable requirements, and instead must carefully examine federal and state data breach notification and other laws, regulations, and requirements in order to assess their potential application to each particular circumstance.

2. For each law and regulation identified in Question 1, please describe:

a. The general scope of the breach notice requirement.

HIPAA’s requirements for breach notice are primarily contained in the Breach Notification Rule (45 C.F.R. §§164.400-414). HIPAA requires notice for certain unauthorized acquisitions, accesses, uses or disclosures of protected health information ("PHI") maintained by a “Covered Entity” (certain health plans, health care clearinghouses, and health care providers covered by HIPAA) or a “Business Associate” (generally, service providers covered by HIPAA that use or access PHI to provide services to or for Covered Entities). PHI consists of identified or identifiable information that: (1) relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual; and (2) is created or received by a health care provider, health plan, employer, or health care clearinghouse. Additional breach notification duties apply to vendors of personal health

GLBA’s breach notice obligations apply to certain financial institutions that provide financial products and services to consumers, and attach primarily to the unauthorized access to or use of “sensitive customer information.” Under GLBA, service providers to financial institutions are not directly subject to the regulation, but the financial institutions are obligated to establish contracts with such entities to require the reporting of breaches to the financial institution.

In general, state breach notification laws may apply in certain circumstances to any entity that owns, maintains, or licenses certain categories of sensitive personal information about a resident of that state. Also, state breach notification laws may also apply to service providers that maintain such sensitive personal information on behalf of the data owner/licensor.

b. The definition or standard of a covered “data breach.”

HIPAA’s breach notice requirements apply to “breaches” of “unsecured protected health information” by Covered Entities and Business Associates. A “breach” is the acquisition, access, use, or disclosure of protected health information in a manner not permitted under HIPAA which compromises the security or privacy of the PHI. “Unsecured protected health information” is PHI that is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified by the Secretary of Health and Human Services. There are specified exclusions or exceptions to the application of the breach notification requirements, such as if: (i) the PHI was protected by encryption with specified security (and no compromise of the key) (e.g., is not “unsecured protected health information”); (ii) there is a low probability that the information has been compromised taking into account specified criteria (as provided in more detail below) (“Low Probability of Compromise Exception”); or (iii) the information was acquired, accessed, used, or disclosed by an employee/agent of a Covered Entity or Business Associate for a legitimate purpose and there is no further unauthorized use or disclosure of that information (“Good Faith Exception”). When analyzing a breach to determine whether the Low Probability of Compromise Exception applies, Covered Entities and Business Associates must consider at least the following four factors: (1) the nature and extent of the PHI involved, including the likelihood data could be reidentified; (2) the unauthorized person who used PHI or to whom an improper disclosure was made; (3) whether the PHI was actually acquired or viewed; and (4) the extent to which the risk to the PHI was mitigated.

GLBA’s breach notice requirement applies to the unauthorized access to or use of “sensitive customer information,” which includes an individual’s name, address, or telephone number in conjunction with the individual’s: (1) Social
Data Breach Notification Guide

Security Number; (2) driver’s license number; (3) account number; (4) credit or debit card number; or (5) personal identification number, password or any combination of customer information that would permit access to a customer’s account. GLBA similarly provides a harm-based exception to the breach notice obligation if the entity reasonably determines that misuse of the information has not and is not likely to occur.

At the state level, the definition of a data breach varies across states. Specifically, for purposes of illustration, note the circumstances under which the following states’ breach notice laws may apply:

- **California.** Generally covers the unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the person or business. The categories of personal information covered by the law include: an individual’s first name or initial and last name in combination with any of the following, when either the name or the following are unencrypted: (1) Social Security Number; (2) driver’s license number or California identification card number; (3) account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual’s financial account; (4) medical information; (5) health insurance information; or (6) information or data collected through the use or operation of an “automated license plate recognition system.” The breach notification law also covers an individual’s user name or email address, in combination with a password or security question and answer that would permit access to an online account.

- **District of Columbia.** Generally covers the unauthorized acquisition of computerized or other electronic data, or any equipment or device storing such data, which compromises the security, confidentiality, or integrity of personal information maintained by the person or business. The categories of personal information covered by the law include: an individual’s first name or initial and last name, phone number or address, in combination with any of the following, when either the name or the following are unencrypted: (1) Social Security Number; (2) driver’s license or District of Columbia identification card number; or (3) credit or debit card number. The breach notification law also covers any other number, code or combination of numbers or codes, such as account number, security code, access code, or password that allows access to or use of an individual’s financial or credit account.

- **Florida.** Generally covers the unauthorized access of data in electronic form containing personal information. The categories of personal information covered by the law include: an individual’s first name or initial and last name in combination with any of the following, when either the
name or the following are unencrypted: (1) Social Security Number; (2) driver’s license or identification card number, passport number, military identification number, or other similar number issued on a government document used to verify identity; (3) financial account number or credit or debit card number, in combination with any required security code, access code, or password that is necessary to permit access to an individual’s financial account; (4) medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional; (5) health insurance policy number or subscriber identification number and any unique identifier used by a health insurer to identify the individual; or (6) user name or email address, in combination with a password or security question and answer that would permit access to an online account.

- **Illinois.** Generally covers the unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the data collector. The categories of personal information covered by the rule include: an individual’s first name or initial and last name in combination with any of the following, when either the name or the following are not encrypted or redacted, or effective January 2017, are encrypted or redacted but the keys to unencrypt or unredact have also been acquired: (1) Social Security Number; (2) driver’s license number or state identification card number; or (3) account number, credit or debit card number, in combination with any required security code, access code that would permit access to an individual’s account; (4) medical information (effective January 2017); (5) health insurance information (effective January 2017); and (6) Unique biometric data (e.g., fingerprint, retina or iris image) (effective January 2017). Also effective January 2017, the breach notification law will cover an individual’s user name or email address, in combination with a password or security question and answer that would permit access to an online account when this information is not encrypted or redacted, or is encrypted or redacted but the keys to unencrypt or unredact have also been acquired.

- **Massachusetts.** Generally covers the unauthorized acquisition or unauthorized use of unencrypted data or, encrypted electronic data and the confidential process or key that is capable of compromising the security, confidentiality, or integrity of personal information, maintained by a person or agency that creates a substantial risk of identity theft or fraud against a resident of Massachusetts. The categories of personal information covered by the law include: an individual’s first name and last name or first initial and last name in combination with any of the following: (1) Social Security Number; (2) driver’s license number or state-issued identification card number; or (3) financial account number, or credit or debit card number, with or without any required security code, access
code, personal identification number or password, that would permit
access to the individual’s financial account.

- **New York.** Generally covers the unauthorized acquisition or acquisition
  without valid authorization of computerized data that compromises the
  security, confidentiality, or integrity of personal information maintained by
  a business. The categories of personal information covered by the law
  include any information that could be used to identify a natural person in
  combination with any of the following, when either the name or the
  following are unencrypted, or encrypted with an encryption key that has
  also been acquired: (1) Social Security Number; (2) driver’s license
  number or non-driver identification card number; or (3) account number,
  credit or debit card number, in combination with any required security
  code, access code or password that would permit access to an
  individual’s financial account.

- **Texas.** Generally covers the unauthorized acquisition of computerized
  data that compromises the security, confidentiality, or integrity of sensitive
  personal information maintained by a person. The categories of personal
  information covered by the law include: an individual’s first name or initial
  and last name in combination with any of the following, when the name
  and the following are unencrypted, or encrypted with an encryption key
  that has also been acquired: (1) Social Security Number; (2) driver’s
  license number or government issued identification number; or (3)
  account number, credit or debit card number, in combination with any
  required security code, access code or password that would permit
  access to an individual’s financial account. The breach notification law
  also covers information that identifies an individual and relates to his/her:
  (1) physical or mental health condition; (2) provision of healthcare to the
  individual; or (3) payment for the provision of health care to the individual.

c. **Whether it is mandatory to notify affected individuals.**

At both the federal and state level, an entity generally is required to notify
affected individuals if the activities come within the scope of the relevant
breach notification laws, unless an exception or exclusion applies. For HIPAA
and GLBA, see discussion above under the definition or standard of a covered
data breach. For state laws, beyond proper encryption, relevant exceptions or
exclusions for the key states summarized in this guide include the following:

- **California.** The breach notification law may not apply to the good faith
  acquisition of personal information by an employee or agent of the person
  or business for the purposes of the person or business, provided that the
  personal information is not used or subject to further unauthorized
disclosure.
• **District of Columbia.** The breach notification law may not apply to the good faith acquisition of personal information by an employee or agent of the person or business for the purposes of the person or business, if the personal information is not used improperly or subject to further unauthorized disclosure.

• **Florida.** The breach notification law may not apply to the good faith access of personal information by an employee or agent of the covered entity, provided that the information is not used for a purpose unrelated to the business or subject to further unauthorized use. The breach notification law also may not apply if after an appropriate investigation and consultation with relevant federal, state, or local law enforcement agencies, the covered entity reasonably determines that the breach has not and will not likely result in identity theft or any other financial harm to the individuals whose personal information has been accessed.

• **Illinois.** The breach notification law may not apply to the good faith acquisition of personal information by an employee or agent of the data collector for a legitimate purpose of the data collector, provided that the personal information is not used for a purpose unrelated to the data collector’s business or subject to further unauthorized disclosure.

• **Massachusetts.** The breach notification law may not apply to the good faith acquisition of personal information by a person or agency, or employee or agent thereof, for the lawful purposes of such person or agency, unless the personal information is used in an unauthorized manner or subject to further unauthorized disclosure.

• **New York.** The breach notification law may not apply to the good faith acquisition of personal information by an employee or agent of the business for the purposes of the business, if the personal information is not used or subject to unauthorized disclosure.

• **Texas.** The breach notification law may not apply to the good faith acquisition of sensitive personal information by an employee or agent of the person for the purposes of the person, unless the person uses or discloses the sensitive personal information in an unauthorized manner.

d. **Whether it is mandatory to notify any government authorities.**
Under HIPAA, if more than 500 individuals are affected by a breach, a Covered Entity must notify the Secretary of Health and Human Services “without unreasonable delay” and in no case later than 60 days of discovering the breach of PHI. If fewer than 500 individuals are affected, notice to the Secretary of Health and Human Services must be provided within 60 days of the end of the calendar year.
Financial institutions covered under GLBA are required to notify their primary federal regulator.

At the state level, approximately 23 states impose duties to notify state authorities under specified conditions, and in some instances, subject to timing requirements (e.g., some states require notification to state authorities prior to notifying individuals). Specifically, note the following government reporting obligations for the key states summarized in this guide:

- **California.** Notice to the California Attorney General’s Office is required if more than 500 residents are impacted by the data breach.

- **District of Columbia.** No mandatory reporting to a government agency.

- **Florida.** Notice to the Department of Legal Affairs is required if more than 500 residents are impacted by the data breach.

- **Illinois.** No mandatory reporting to a government agency.

- **Massachusetts.** Notice to the Massachusetts Attorney General, Director of Consumer Affairs and Business Regulation, and any other state agencies that the Director might specify to receive notice is required concurrent with any notice to residents.


- **Texas.** No mandatory reporting to a government agency.

- **Whether any other parties may need to be notified of the incident.**

Under HIPAA, a Covered Entity may be required to notify the media if more than 500 individuals are affected, and under GLBA, financial institutions are encouraged to report to nationwide consumer reporting agencies prior to sending notices to large numbers of customers.

At the state level, an entity may be required to notify all consumer reporting agencies if a certain number of individuals (e.g., 1,000) across the United States or in a particular state are affected by the data breach. Also, depending on the method of notice (e.g., substitute notice), it may be necessary to provide additional forms of notice, such as posting a notification on the entity’s public website or communicating the notice to statewide media. Specifically, beyond substitute notice situations, note the obligations to notify consumer reporting agencies for the key states summarized in this guide:

- **California.** No mandatory duty to report to consumer reporting agencies.
• **District of Columbia.** Appropriate credit reporting agencies must be notified of the data breach if more than 1,000 individuals must be notified.

• **Florida.** Appropriate credit reporting agencies must be notified of the data breach if more than 1,000 individuals must be notified at one time.

• **Illinois.** No mandatory duty to report to consumer reporting agencies.

• **Massachusetts.** No statutory duty to report to consumer reporting agencies, unless so directed by the Director of Consumer Affairs and Business Regulation.

• **New York.** Appropriate credit reporting agencies must be notified of the data breach if more than 5,000 New York residents must be notified at one time.

• **Texas.** Appropriate credit reporting agencies must be notified of the data breach if more than 10,000 individuals must be notified at one time.

f. **Whether the above rules are different if the company is acting as a data processor/service provider, and not acting as the data controller/owner of the information at issue.**

At both the federal and state level, the obligation to notify individuals, government authorities and non-government parties usually rests with the entity that “owns/licenses” the personal information. Thus, at the federal level, the obligation to notify the above parties of a data breach rests with the Covered Entity, not the Business Associate, under HIPAA, and the financial institution covered by the GLBA, not its service provider. If the Business Associate or service provider experiences the data breach, it is obligated to notify the Covered Entity or financial institution at issue (not the individuals or government authorities).

At the state level, the obligation to notify the above parties similarly rests with the entity that “owns/licenses” the personal information that was subject to the breach. Service providers that maintain personal information on behalf of the entity that “owns/licenses” the personal information are generally required to notify that entity (not the individuals or government authorities). However, in some cases it is possible for the parties to agree via contract that the service provider is responsible for notifying affected individuals and otherwise complying with applicable data breach notice requirements. In spite of such agreements, however, the entity that “owns/licenses” the personal information will be remain legally responsible for compliance with the relevant breach notification laws.
g. What are the potential penalties for non-compliance with the breach notice obligation?

Violation of HIPAA’s breach notice requirements could result in civil money penalties of up to $1.5 million per violation and settlement agreements that include mandated corrective actions and monitoring for Covered Entities and Business Associates, along with imprisonment for egregious violations. Violations of GLBA’s breach notice requirements could similarly result in civil penalties and sanctions, including fines and other consequences that vary depending on the responsible regulatory authority.

With regard to state breach notification laws, note for illustration purposes the penalties for the key states summarized in this guide:

- **California.** Penalties include a private action to recover damages, civil penalties up to $3,000 per violation, and/or injunctive relief.
- **District of Columbia.** Penalties include a private action to recover damages, civil penalties up to $100 per violation, and/or injunctive relief.
- **Florida.** Penalties include a civil penalty up to $50,000 per 30 day period in violation of the breach law (not to exceed $500,000), and/or injunctive relief.
- **Illinois.** Penalties include a private action to recover damages, civil penalties up to $50,000 per violation, and/or injunctive relief.
- **Massachusetts.** Penalties include civil penalties of up to $5,000 per violation, as well as reasonable costs of investigation and litigation of the violation.
- **New York.** Penalties include civil penalties up to the greater of $5,000 or $10 per failed notice (not to exceed $150,000), and/or injunctive relief.
- **Texas.** Penalties include civil penalties up to $50,000 per violation in addition to up to $100 per individual per day for failed breach notice, and/or injunctive relief.

***

In addition, beyond regulatory penalties associated with failure to comply with breach notification requirements, the consequences for data breaches in the United States can be significant and include: private rights of action, such as class actions by consumers, financial institutions, business partners, or shareholder derivative suits; regulatory actions for underlying data security issues; customer churn and revenue loss; adverse media attention and reputational harm; and other consequences.
Uruguay

**Martin Pesce**
Montevideo
Tel: +598 2900 1000 ext. 7982
mpesce@ferrere.com

**Santiago Dutra**
Montevideo
Tel: +598 2900 1000 ext. 1610
sdutra@ferrere.com
1. In your jurisdiction, are there legal requirements for organizations to provide notice of a breach of security for personal data or other company information?

Yes.

Please identify the name of the relevant law(s) or regulation(s).

- Decree 414/2009, regulatory of Law 18.331 on Data Privacy.

2. For each law and regulation identified in Question 1, please describe:

a. The general scope of the breach notice requirement.

The regulation makes no distinction on the types of data, the industry sector or company-type.

However, when the breach is related to sensitive data, it is more likely to significantly affect the rights of data subjects.

b. The definition or standard of a covered “data breach.”

The notice is required where the security incident is likely to significantly affect the rights of the data subjects.

The Local Data Privacy Authority has not established to date which breaches may be deemed to substantially affect data subjects. As such, the determination of whether the notification is required or not must be carried out by the data controller itself.

Notwithstanding the above, we point out that during informal communications with the local regulator, we were informed that those types of breaches would be related to sensitive data, or confidential information, or cases where the breach did not involve those types of data but lasted for a relevant period of time.

c. Whether it is mandatory to notify affected individuals.

Yes.

There is no standard regarding the time and content of the notification.

d. Whether it is mandatory to notify any government authorities.

No.

e. Whether any other parties may need to be notified of the incident.

Yes.
If the breach occurs to a company acting as a data processor, it is typical for the data processing contracts to determine the obligation to notify the data controller, since the latter is responsible to the data subjects and the Local Data Privacy Authority for the information.

f. Whether the above rules are different if the company is acting as a data processor/service provider, and not acting as the data controller/owner of the information at issue.

No.

g. What are the potential penalties for non-compliance with the breach notice obligation?

Penalties for the failure to notify are not specifically determined; however said failure (when notification was indeed required) would be deemed an infringement of the data protection law. Infringements to the law may be penalized by observations, warnings, fines up to USD 55,000, or even the closure of the database when the infringement is deemed to be very relevant, in which case the intention of the sanctioned party (among other aspects) will be taken into account to determine the penalty.
Vietnam

Yee Chung Seck
Ho Chi Minh City
Tel: +84 8 829 6234
yeechung.seck@bakermckenzie.com

Minh Tri Quach
Hanoi
Tel: +84 4 3936 9605
minhtri.quach@bmvn.com.vn
1. In your jurisdiction, are there legal requirements for organizations to provide notice of a breach of security for personal data or other company information?

Yes.

**Please identify the name of the relevant law(s) or regulation(s).**

Decree 52/2013/ND-CP; Circular No. 27/2011/TT-BTTTT

2. For each law and regulation identified in Question 1, please describe:

a. **The general scope of the breach notice requirement.**

   In the e-commerce context: Vietnamese law requires that, if an information system is hacked in a way that poses a risk of loss of consumer information, the information storing organization shall notify the incident to a functional agency within 24 (twenty-four) hours after detecting it. (Decree 52/2013/ND-CP, Article 72). Generally and in any context and for any type of information, organizations and individuals must report “Internet incidents” that they are unable to handle on their own to one or more of the following members of the incident response network: the network member responsible for incident response for that user (if any), the ISP that directly supplies Internet services to the user, and/or the Vietnam Computer Emergency Response Team (VNCERT). (Circular No. 27/2011/TT-BTTTT). For “serious Internet incidents,” generally in any context and for any type of information, Circular 27 requires immediate reporting to VNCERT. Serious incidents include those that occur on a large scale, spread quickly, threaten serious harm to computer and Internet network systems, cause serious loss of information or which require substantial national or international resources to resolve. (Circular No. 27/2011/TT-BTTTT).

b. **The definition or standard of a covered “data breach.”**

   Under Circular 27, an “Internet incident” that requires reporting, means an event which has occurred, is occurring or is likely to occur, causes information insecurity on the Internet, and is detected through supervision, evaluation and analysis of concerned agencies, organizations or persons or warned by domestic or foreign information security specialists or organizations. Under Circular 27, a “serious Internet incident” which requires immediate reporting, means an incident with one or more of the following properties: likely spreading wide and fast; likely destroying computer networks and the Internet; likely causing major damage or consequences to communication systems on the network; and requiring coordinated major national or international resources for settlement.
c. Whether it is mandatory to notify affected individuals.
No.

d. Whether it is mandatory to notify any government authorities.
Yes.

In the e-commerce context: Vietnamese law requires that, if an information system is hacked in a way that poses a risk of loss of consumer information, the information storing organization shall notify the incident to a functional agency within 24 (twenty-four) hours after detecting it. (Decree 52/2013/ND-CP, Article 72). Generally and in any context and for any type of information, organizations and individuals must report “Internet incidents” that they are unable to handle on their own to one or more of the following members of the incident response network: the network member responsible for incident response for that user (if any), the ISP that directly supplies Internet services to the user, and/or the Vietnam Computer Emergency Response Team (VNCERT). (Circular No. 27/2011/TT-BTTTT). For “serious Internet incidents”, generally in any context and for any type of information, Circular 27 requires immediate reporting to VNCERT. Serious incidents include those that occur on a large scale, spread quickly, threaten serious harm to computer and Internet network systems, cause serious loss of information or which require substantial national or international resources to resolve. (Circular No. 27/2011/TT-BTTTT).

e. Whether any other parties may need to be notified of the incident.
Yes.

In the e-commerce context: Vietnamese law requires that, if an information system is hacked in a way that poses a risk of loss of consumer information, the information storing organization shall notify the incident to a functional agency within 24 (twenty-four) hours after detecting it. (Decree 52/2013/ND-CP, Article 72). Generally and in any context and for any type of information, organizations and individuals must report “Internet incidents” that they are unable to handle on their own to one or more of the following members of the incident response network: the network member responsible for incident response for that user (if any), the ISP that directly supplies Internet services to the user, and/or the Vietnam Computer Emergency Response Team (VNCERT). (Circular No. 27/2011/TT-BTTTT). For “serious Internet incidents”, generally in any context and for any type of information, Circular 27 requires immediate reporting to VNCERT. Serious incidents include those that occur on a large scale, spread quickly, threaten serious harm to computer and Internet network systems, cause serious loss of information or which require substantial national or international resources to resolve. (Circular No. 27/2011/TT-BTTTT).
f. Whether the above rules are different if the company is acting as a data processor/service provider, and not acting as the data controller/owner of the information at issue.

No.

g. What are the potential penalties for non-compliance with the breach notice obligation?

Failure to comply with the above reporting requirements above may result in fines of up to VND30 million (approx. USD 1,500) (Article 71.3(a) and (b) of Decree 174/2013/ND-CP) per incident.
Baker & McKenzie Offices Worldwide

Office phone numbers and addresses change from time to time. Please refer to www.bakermckenzie.com for current contact information.
Baker & McKenzie has been global since inception. Being global is part of our DNA.

Our difference is the way we think, work and behave – we combine an instinctively global perspective with a genuinely multicultural approach, enabled by collaborative relationships and yielding practical, innovative advice. Serving our clients with more than 4,200 lawyers in more than 45 countries, we have a deep understanding of the culture of business the world over and are able to bring the talent and experience needed to navigate complexity across practices and borders with ease.