



# **A Global Landscape :** Data Breach Notification Requirements Across Countries

# Contributing experts

## Argentina

10 Mariano Peruzzotti  
OJAMBF

## Australia

11 Kelly Dickson -  
Macpherson Kelley

## Austria

13 Dr. Gerald Trieb, LL.M. -  
Knyrim Trieb Attorneys

## Brazil

16 Luiza Sato -  
TozziniFreire  
Advogados

## Canada

18 Lyndsay A. Wasser -  
McMillan

## China

20 Richard Ma -  
DaHui Lawyers

## Colombia

21 Andrea Garzon -  
Vanegas Morales

## Finland

23 Erika Leinonen -  
Lexia Attorneys

## France

25 Jean-Christophe  
Chevallier - Ydès

## Hong Kong

27 Pádraig Walsh -  
Tanner de Witt

## Hungary

29 Endre Várady- VJT &  
Partners

## India

31 Arun Babu - Kochhar &  
Co

## Italy

33 Luca Egitto-  
RPLT

## Japan

35 Akira Matsuda - Iwata  
Godo

## Netherlands

37 Stephan Mulders -  
Van Diepen Van der  
Kroef Advocaten

## Norway

39 Alexander Mollan -  
Brækhus  
Advokatfirma DA

## Singapore

41 Winnie Chang -  
OrionW

## Spain

43 Beatriz Rodríguez  
Gómez - RocaJunyent

## Taiwan

45 John Eastwood -  
Eiger

## Türkiye

47 Ozan Karaduman -  
Karaduman &

## Ukraine

49 Oksana Zadniprovska  
- AXON Partners

## UK

51 Kim Walker -  
Shakespeare  
Martineau LLP

## USA

53 Gene Price - Frost  
Brown Todd



# A Global Landscape :

# Data Breach Notification Requirements Across Countries

In an increasingly digital world, people and organizations have become much more interconnected. This gives rise to significant benefits, including allowing organizations to find partners across the globe, as well as providing individuals with access to a broader range of products and services. However, it also means that more data is flowing across borders than ever before. This being the case, when a data breach occurs there are often a number of national and local laws that may apply to the incident. To avoid significant penalties and reputational damage, it is critical for organizations to obtain sophisticated advice from experts in all jurisdictions where relevant data subjects are located. PrivacyRules offers a network of trusted advisors, who can guide organizations through complex data breaches, including by coordinating with local counsel in multiple jurisdictions.



**Lyndsay A. Wasser**  
Chair of the PrivacyRules Data Breach Committee

## Introduction

The size, scope, and frequency of data breaches have increased exponentially in recent years as a result of the growing adoption of digital platforms by organizations of any kind. Governments worldwide have enacted legislation and protocols for incident response. Most of these frameworks require prompt notification to designated authorities and affected individuals to mitigate the potential harm from data breaches.

A significant number of countries have implemented data breach notification requirements. Among them we have listed Argentina, Australia, Austria, Brazil, Canada, China, Colombia, Finland, France, Hong Kong, Hungary, India, Italy, Japan, the Netherlands, Norway, Singapore, Spain, Taiwan, Türkiye, Ukraine, the United Kingdom, and the United States of America.

It is widely recognised that the most efficient and cost effective data breach response starts with a solid prevention plan. National laws are becoming more stringent on the obligation of organisations to implement cyber security measures, while also demanding greater transparency in the event of a breach. They typically include pressing notification requirements and deadlines which cannot be properly handled without accurate preparation.



To help organisations navigate this intricate scenario, especially when they process and transfer data to multiple jurisdictions, the PrivacyRules alliance has created coordinated services availing the in-depth expertise of its legal, cybersecurity, and crisis communications experts to face any phase of a data breach locally and internationally. Our services span from data crisis preparedness to recovery and business continuity.

Read on to find out more, and feel free to contact us for a bespoke assessment. We are ready to support clients of any size 24/7/365, while we underline that the best response starts from an efficient prevention and preparedness strategy.

**Alessandro Di Mattia**  
Director of the PrivacyRules Alliance

# A Global Landscape :

## Data Breach Notification Requirements Across Countries

### Exploring Data Breach Notification Triggers Around the World

Data breach notification requirements vary significantly, with some countries mandating notification for all breaches, while others focus on breaches with a high risk of harm.

**1. Risk-based approach : Argentina, Australia, Canada, Colombia and European countries** generally require notification only if the breach is likely to result in a high risk of harm to individuals (e.g., identity theft, financial loss, damage to reputation).

**2. Specific criteria :** The law in Japan focuses on specific criteria for notifications, such as breaches affecting more than 1,000 individuals, and both Japan and Taiwan prescribe obligations for breaches affecting certain organisations (such as critical infrastructure providers or public entities) or involving specific data types (e.g., sensitive data)

**India** prioritizes national security and personal data protection by requiring notification for any breach impacting public information infrastructure.

**Brazil** has specific criteria for an eligible data breach , as follows::

- **Significant impact on data subjects:** The breach must significantly affect the data subjects' interests and fundamental rights, either by preventing the exercise of rights or causing material or moral damage.
- **Involvement of specific data categories:** The breach must involve at least one of the following categories of data: sensitive personal data, data relating to children, adolescents or the elderly, financial data, system authentication data, data protected by legal, judicial or professional secrecy, or large-scale processed data.

**In the United States** Organizations must notify affected individuals if unencrypted personal information is compromised due to unauthorized access, or if encrypted information is compromised along with the encryption key. The breach must involve specific categories of personal information like social security numbers, driver's license numbers, or medical data.

**In Canada,** Federal legislation applicable to commercial activities requires notification of affected individuals if a breach of security safeguards gives rise to a real risk of significant harm. The threshold for reporting under provincial legislation and sector-specific legislation and regulatory requirements varies across the country.

**3. Broad criteria: India** mandates reporting any data breach to the Indian Computer Emergency Response Team (CERT-In). **Hungary** takes a similar approach, requiring notification for almost any breach to the local DPA.

To note: **Hong Kong's** notification requirement is not mandatory, but the Office of the Privacy Commissioner for Personal Data (PCPD) strongly recommends notification after becoming aware of a data breach when it poses a real risk of harm to individuals. **Ukraine's** system is currently unclear for personal data, focusing on unauthorized access to state information.

# A Global Landscape :

## Data Breach Notification Requirements Across Countries

### When to Notify Individuals of a Data Breach: A Global Comparison

GDPR-based countries, like Austria, Finland, France, Norway, and Spain, have a **two-tiered system**: authorities are notified for most breaches, while individuals are notified only in high-risk situations. This is also the case under some Canadian data protection statutes that apply to certain sectors and/or jurisdictions.

With respect to data breach notification of impacted individuals, most countries (except Hong Kong) require notification to impacted individuals when the data breach poses a risk of harm. The specific risk threshold varies:

- 1. GDPR model, two-tier systems: Other than EU countries also China and Colombia** adopt a GDPR-inspired approach, notifying authorities for most breaches but individuals only in high-risk scenarios.
- 2. High-risk focus: Brazil, Türkiye, USA, and The UK** align closely with the GDPR's high-risk threshold for notifying individuals
- 3. Varying thresholds: Australia** mandates notification for serious risks, while **Japan** requires it for incidents posing a risk of harm. **Argentina** also generally requires notification for breaches that pose a **serious risk** to individuals.

**Netherlands and Brazil both prioritize breaches that pose a serious risk to individuals.** Organizations must take remedial action to contain the breach and mitigate potential harm. If serious harm cannot be mitigated, organizations must notify affected individuals. If direct notification is impractical, organizations must publish a statement on their website and take reasonable steps to inform individuals at risk.

**In Canada**, the threshold for reporting varies across jurisdictions and sectors. The legislation applicable to interprovincial and international processing of personal information in the course of commercial activities requires notification if individuals are at real risk of significant harm.

- 4. Dual approach: India** requires reporting all cybersecurity incidents to CERT-In. The new DPDPA will require notification to individuals for all data breaches. **Taiwan** requires notification to authorities and individuals for breaches involving sensitive data or a large number of individuals

### Beyond Individual Notices: Alternative Measures for Data Breaches

In some countries, notifying every affected individual directly may not be feasible or effective in all data breach scenarios. The concept of "impractical individual notification" allows for alternative measures when direct notification is not practical.



# A Global Landscape :

## Data Breach Notification Requirements Across Countries

### Alternative Measures:

- **Public Statements:** Countries like **Australia** allow public statements to inform individuals when direct notification is impractical. Some statutes in Canada also require indirect notifications, such as public statements, when direct notifications are not possible and/or if certain other conditions are met.
- **CNIL Assessment:** In **France** the CNIL can assess the effectiveness of chosen notification methods, considering practicality.
- **Website Statements and Public Awareness:** The TKDK and AP in **Türkiye** and **the Netherlands** may require website statements and public awareness efforts for high-risk breaches.

**Hungary** uses the ENISA methodology score to assess notification needs, a less common approach in other EU countries.

### Data Breach Notification Deadlines

While there's some variation across countries, most emphasize notifying authorities promptly. The 72-hour timeframe is a common standard seen in many countries aligned with the GDPR framework. We might categorize the deadlines into 3 main categories:

**1.. Strict 72-hour timeframe:** This group aligns with the GDPR framework and reflects a clear deadline for notifying authorities. (**Austria, Hungary, Finland, Norway, Netherlands, Türkiye, UK**)

#### 2. Specific Timeframes :

**Taiwan** within an hour

**Colombia** has a clear deadline of 15 working days for reporting to the competent authority.

**Japan** has a two part reporting process:

- Initial report: needs to be submitted within 3-5 days of discovering the breach.
- Final report: Needs to be submitted within 30-60 days of discovering the breach.

#### **Brazil**

- The data subjects and the ANPD must be notified within 3 business days after the controller becomes aware that the incident has impacted personal data, except when a communication deadline is established by specific legislation.
- The ANPD may, at any time, request additional information from the controller
- Deadlines are doubled for small-scale agents

**3. As Soon as Practicable:** This group emphasizes prompt notification but doesn't specify a strict deadline. Some countries within this group offer additional guidance or suggestions. For example, **Brazil** suggests two days of time. **Australia** (after an assessment is done).

In both **The United States and Canada** the timeline for notifying impacted individuals can vary across sectors and jurisdictions. However, for businesses that are not healthcare custodians, in Canada individuals generally need to be notified as soon as feasible after the organization discovers a data breach.

# A Global Landscape :

## Data Breach Notification Requirements Across Countries

**4. No specific timing requirement:** **China** has no specific timing requirement in the relevant legislation, but immediate notification to competent authorities is mandated

**India has Currently No Mandatory Notification** but the upcoming Data Protection Bill is expected to introduce specific requirements.

**Spain and France:** Both countries prioritize prompt notification but do not mandate a specific timeframe. Spain's regulations lean towards a flexible approach, emphasizing promptness without a strict deadline.

### Stricter National Documentation Requirements in the EU

The General Data Protection Regulation (GDPR) sets a baseline for data protection across Europe. But some EU member states can add stricter national laws on top of the GDPR. These stricter laws often involve additional documentation requirements for data breaches.

#### France and Spain:

- Require organizations to document all data breaches, regardless of whether they need to be reported to the authorities.
- Even minor incidents, like accidental email disclosures, need to be documented
- Stricter requirements apply to the content of this documentation (i.e., as compared to the GDPR), including requirements for specific details for each breach (e.g., type of breach, data affected, number of individuals impacted).

**Netherlands and Austria** documentation is likely required for all breaches as well. However, the specific details organizations need to document might be less defined compared to France and Spain.

To note: **In India, there is a two-step approach:**

- **National "Directions":** This is a general framework outlining data breach reporting requirements for most organizations in India.
- **Sector-Specific Regulations:** Additionally, specific regulations exist for certain industries like banking, payments, securities, and insurance. These industries likely have stricter requirements for documenting and reporting data breaches.

# A Global Landscape :

## Data Breach Notification Requirements Across Countries

### Data Breach Notification and Recordkeeping in Canada and USA: A Complex Landscape

**Canada** : Canadian organizations must navigate a complex network of federal, provincial, and sector-specific requirements for data breach reporting, notifications and recordkeeping.

#### Federal Level (Private Sector):

- The Personal Information Protection and Electronic Documents Act applies to personal information that is processed in the course of interprovincial and international commercial activities, as well as commercial activities in provinces that do not have substantially similar legislation. It also applies to employee personal information for federally-regulated works, undertakings and businesses.
- Organizations must report breaches of security safeguards that give rise to a real risk of significant harm to relevant individuals, the Office of the Privacy Commissioner of Canada, and any other organization or governmental institution (or part thereof) that may be able to reduce or mitigate the risk of harm.
- Organizations must maintain a record of every breach of security safeguards for 24 months.
- Federally regulated financial institutions must report technology and cybersecurity incidents to the Office of the Superintendent of Financial Institutions.

#### Provincial Level (Private Sector):

- Alberta's Personal Information Protection Act requires that breaches must be reported to the regulator if they give rise to a real risk of significant harm, and the regulator may require notification of impacted individuals.
- Quebec's Act respecting the protection of personal information in the private sector requires notification of individuals and the regulator if a confidentiality incident presents a risk of serious injury, and it requires that organizations must keep a record of all confidentiality incidents for five (5) years (the content of which is prescribed by regulation).
- Some data protection statutes that apply to certain health information custodians also include breach reporting obligations.

#### Public Sector:

- Certain statutes governing protection of personal information by public bodies and institutions also include breach reporting requirements.

#### Sector-Specific Requirements:

- The regulators for certain industries require reporting of certain types of breaches or cybersecurity incidents (e.g., OSFI, IIROC).



# A Global Landscape :

## Data Breach Notification Requirements Across Countries

### Unites States (California):

**Notification Methods:** Written or electronic notice is typically required.

**Substitute Notice:** For breaches affecting over 500,000 individuals or costing more than \$250,000, substitute notice may be used.

- Email notification
- Conspicuous website posting for at least 30 days
- Notification to major statewide media

**Healthcare Providers:** Additional rules may apply under the California Health and Safety Code.

Most States also have specific statutes mandating reporting of certain types of breaches. The details vary from State to State.


This brief introduction of the data breach notification requirements across countries has been developed by **Rajaa Dawi, Legal Assistant of the PrivacyRules Alliance.**



# Mariano Peruzzotti

 Argentina

 mperuzzotti@ojambf.com

 +54 (11) 4549-4900

 www.ojambf.com



## Legislation

Personal Data Protection Law No. 25,326 (2000)

## Type(s) of Breach(es)

An eligible data breach occurs when the security incident compromises personal data defined as any kind of information related to an identified or identifiable individual or legal entity.

## Notification to Regulator(s)

Rule No. 47/2018 of the Argentine Data Protection Authority recommends reporting a security incident. The report should contain the following information:

- nature of the breach;
- categories of affected personal data;
- data subjects concerned / affected;
- measures implemented in order to mitigate the breach; and to prevent future incidents.

## Timing for Reporting

N/A

## Reporting Obligation (Y/N)

No

## Threshold for Breach Reporting

N/A

## Communication to Data Subjects

Argentine Law does not impose the obligation of reporting a data breach to the impacted data subjects. Nevertheless, in consideration of Rule No. 47/2018 and the general good faith and damage prevention principles provided in the Argentine Civil and Commercial Code, it will be advisable to notify the affected individuals or legal entities in the event a company becomes aware that a security breach may potentially affect data subjects' rights and interests.

## Other Notification Obligations

N/A

## Additional Notes

Several sectorial regulations may impose reporting duties such as the case of the regulations applicable to the financial industry.

[Back to countries](#) 

# Kelly Dickson



Australia



kelly.dickson@mk.com.au



+61 3 9794 2541



mk.com.au

macpherson kelley.



## Legislation

The Privacy Act 1988 (Cth)

## Type(s) of Breach(es)

An eligible data breach occurs when the following criteria are met:

- a) There is unauthorised access to, or disclosure of, personal information held by an organisation, or information is lost in circumstances where unauthorised access or disclosure is likely to occur;
  - b) This is likely to result in serious harm to any of the individuals to whom the information relates; and
  - c) The organisation has been unable to mitigate the serious harm occurring.
- "Personal Information" means information or an opinion about an individual who is identified, or reasonably identifiable.

"Serious harm" will depend on the kind / sensitivity of the information, "who" has obtained the information, the type and extent of security measures in place, and the nature of the harm.

## Notification to Regulator(s)

Yes. The organisation must report to the OAIC. The report must include:

- the organisation's name and contact details
- a description of the data breach
- the kinds or nature of information involved
- recommendations about the remedial steps individuals should take in response to the data breach

## Timing for Reporting

Organizations subject to the Notifiable Data Breach scheme are required to conduct an assessment of any suspected eligible data breaches and take reasonable steps to complete this assessment within 30 days. Affected organizations must notify individuals as soon as practicable after completing the statement prepared for notifying the OAIC

## Reporting Obligation (Y/N)

Yes

## Threshold for Breach Reporting

When the organisation has reasonable grounds to believe an eligible data breach has occurred, they must promptly notify any relevant individual at risk of serious harm, and notify the Office of the Australian Information Commissioner (OAIC, Australia's federal privacy regulatory body).

## Communication to Data Subjects

The first step is to contain the breach where possible and take remedial action. Where serious harm cannot be mitigated through remedial action, the organisation must notify individuals at risk of serious harm (either by notifying all individuals, or only those individuals at risk of serious harm).

If it is not practicable to notify individuals at risk of serious harm, the organisation must publish a copy of the statement prepared for the OAIC on its website, and take reasonable steps to bring its contents to the attention of individuals at risk of serious harm.


[Back to countries](#) >



# Kelly Dickson

 Australia

 kelly.dickson@mk.com.au

 +61 3 9794 2541

 mk.com.au

macpherson kelley.

## Other Notification Obligations

N/A

## Additional Notes

Examples of data breaches include:

- loss or theft of physical devices (such as laptops and storage devices) or paper records that contain personal information
- unauthorised access to personal information by an employee
- inadvertent disclosure of personal information due to 'human error', for example an email sent to the wrong person
- disclosure of an individual's personal information to a scammer, as a result of inadequate identity verification procedures.

[Back to countries](#) 

# Gerald Trieb



Austria



gt@kt.at



+43 1 909 30 70



www.ttpn.com.ve



## Legislation

Regulation (EU) 2016/679 - General Data Protection Regulation (GDPR), Austrian Data Protection Act.

## Type(s) of Breach(es)

A breach of security can lead to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

According to recital 85 GDPR, a breach may result in physical, material or non-material damage to natural persons such as loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to the natural person concerned.

Personal data means any information relating to an identified or identifiable natural person.

## Notification to Regulator(s)

The controller has to notify the Austrian Data Protection Authority without undue delay and, where feasible, not later than 72 hours after having become aware of it.

The notification can be sent to the Austrian Data Protection Authority via email to dsb@dsb.gv.at with a meaningful subject.

The Austrian Data Protection Authority provides no online form but a (nonbinding) pdf-formular which can be used .

According to Art 33 GDPR, the notification has to at least

- (a) describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;
- (b) communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;
- (c) describe the likely consequences of the personal data breach;
- (d) describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

## Timing for Reporting

The notification and communication have to be done without undue delay, where feasible, not later than 72 hours after having become aware of the security incident.

If it is not possible to provide all of the information within that time, the information should be provided in phases without undue further delay. If the notification to the Austrian Data Protection Authority is not possible within this time, reasons for the delay should be included in the notification.


The Austrian Data Protection Authority usually does not ask for the exact time of the day when the controller became aware of the security incident; indicative facts, which put the authority in the position to check, whether the notification has been timely filed, suffice in practice.

Back to countries >

# Gerald Trieb

 Austria

 gt@kt.at

 +43 1 909 30 70

 www.ttpn.com.ve



## Reporting Obligation (Y/N)

Yes

## Threshold for Breach Reporting

The data controller has to notify the data breach to the Austrian Data Protection Authority unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons.

If the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller also has to communicate the personal data breach to the impacted data subject.

The ENISA risk assessment methodology or the Art 29 Data Protection Working Party risk assessment methodology can be used to determine the risks to the rights and freedoms of natural persons.

## Communication to Data Subjects

The controller has to communicate the data breach to the data subject without undue delay.

According to Art 34 GDPR, the communication has to describe in clear and plain language

- (a) the nature of the personal data breach ;
- (b) communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;
- (c) describe the likely consequences of the personal data breach;
- (d) describe the measures taken or proposed to be taken by the controller (to address the personal data breach, including where

appropriate, measures to mitigate its possible adverse effects.

The communication to the data subject is not required if

- (a) the controller has implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach, or
- (b) the controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects is no longer likely to materialise or
- (c) it would involve disproportionate effort (though this exception has to be interpreted narrowly). In such a case, there has to instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner.

## Other Notification Obligations

N/A

## Additional Notes

The GDPR also applies to the processing of personal data of data subjects who are in the EU by a controller or processor not established in the EU, where the processing activities are related to:

- (a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the EU; or
  - (b) the monitoring of their behaviour as far as their behaviour takes place within the EU.
- Even if the Austrian Data Protection Authority is not notified about the data breach (as the breach is unlikely to result in a risk to the rights and freedoms of natural persons), the controller is required to document the breach, comprising the facts relating to the


[Back to countries](#) 



## Gerald Trieb

 Austria

 gt@kt.at

 +43 1 909 30 70

 www.ttpn.com.ve



personal data breach, its effects and the remedial action taken, according to Art 33 para 5 GDPR, according to which a register of all respective incidents (also those which have been notified to the supervisory authority) must be listed.

[Back to countries](#) 

# Luiza Sato



Brazil



sato@tozzinifreire.com.br



(5511) 5086-5124



www.tozzinifreire.com.br



## Legislation

Law No. 13,709/2018 (LGPD)  
Resolution ANPD No. 15/2024

## Type(s) of Breach(es)

An eligible data breach occurs when the 2 following criteria are met:

1 - It significantly affects the data subjects' interests and fundamental rights (because it prevents the exercise of rights or the use of a service or because it causes material or moral damage to the data subjects)

AND

2 - It involves at least one of the following categories of data: (i) sensitive personal data; data relating to children, adolescents or the elderly; financial data; system authentication data; data protected by legal, judicial or professional secrecy; and/or (ii) large-scale processed data

## Notification to Regulator(s)

The report must include:

- I - the description of the nature and category of the affected personal data;
- II - the number of affected data subjects, specifying, when applicable, the number of children, adolescents, or elderly individuals;
- III - the technical and security measures used for the protection of personal data, adopted before and after the incident, while observing trade and industrial secrets;
- IV - the risks related to the incident with the identification of possible impacts on the data subjects;

V - the reasons for the delay, in case the communication was not made within the period provided in the main clause of this article;

VI - the measures that have been or will be adopted to reverse or mitigate the effects of the incident on the data subjects;

VII - the date of the incident, when it can be determined, and the date it was known by the controller;

VIII - the data of the data protection officer or the representative of the controller;

IX - the identification of the controller and, if applicable, a statement that it is a small-scale processing agent;

X - the identification of the processor, when applicable;

XI - the description of the incident, including the root cause, if it can be identified; and

XII - the total number of data subjects whose data are processed in the processing activities affected by the incident.

## Timing for Reporting

The data subjects and the ANPD must be notified within 3 business days after the controller becomes aware that the incident has impacted personal data, except when a communication deadline is established by specific legislation

## Reporting Obligation (Y/N)

Yes, in certain cases

[Back to countries](#) >

Luiza Sato



Brazil



sato@tozzinifreire.com.br



(5511) 5086-5124



www.tozzinifreire.com.br



### Threshold for Breach Reporting

When the organisation has **reasonable grounds** to believe an eligible data breach has occurred, they must promptly notify **both the affected data subjects and the ANPD**. The ANPD has a specific channel for receiving such notifications at [https://www.gov.br/anpd/pt-br/canais\\_atendimento/peticionamento-eletronico-anpd](https://www.gov.br/anpd/pt-br/canais_atendimento/peticionamento-eletronico-anpd).

### Communication to Data Subjects

The communication of a security incident to the data subject shall contain the following information:

I - the description of the nature and category of the affected personal data;

II - the technical and security measures used for the protection of the data, while observing trade and industrial secrets;

III - the risks related to the incident with the identification of possible impacts on the data subjects;

IV - the reasons for the delay, in case the communication was not made within the timeframe provided in the main clause of this article;

V - the measures that have been or will be adopted to reverse or mitigate the effects of the incident, when applicable;

VI - the date when the security incident became known; and

VII - the contact information for obtaining further details and, when applicable, the contact details of the data protection officer.

The communication must use simple and easy-to-understand language; and occur in a direct and individualized manner, if it is possible to identify them. If direct and individualized communication is unfeasible or it is not possible to partially or fully identify the affected data subjects, the controller shall communicate the occurrence of the incident through the available dissemination means, such as its website, applications, social media, and data subject service channels, in such a way that the communication allows for broad awareness, with direct and easy visibility, for a period of at least three months.

### Other Notification Obligations

N/A

### Additional Notes

It is up to the controller to request the ANPD, in a reasoned manner, to keep confidential information protected by law, indicating those which access should be restricted.

The ANPD may, at any time, request additional information from the controller, including the records of the processing operations of the personal data affected by the incident, the data protection impact assessment and the report on the treatment of the incident.

Deadlines are doubled for small-scale agents.


Back to countries >



# Lyndsay A. Wasser

 Canada

 lyndsay.wasser@mcmillan.ca

 +1 416.865.7083

 mcmillan.ca



## Legislation

Personal Information Protection and Electronic Documents Act, SC 2000, c 5 ("PIPEDA")

## Type(s) of Breach(es)

Loss of, or unauthorized access to or disclosure of "personal information" resulting from a breach of (or failure to establish) the physical, technological and/or organizational security safeguards required by PIPEDA. "Personal Information" means information about an identifiable individual.

## Notification to Regulator(s)

Yes. The organization must report to the Office of the Privacy Commissioner of Canada. The report must be in writing and include: (a) a description of the circumstances of the breach and, if known, the cause; (b) the day on which, or the period during which, the breach occurred or, if neither is known, the approximate period; (c) a description of the personal information that is the subject of the breach to the extent known; (d) the number of individuals affected by the breach or, if unknown, the approximate number; (e) a description of the steps that the organization has taken to reduce the risk of harm to affected individuals, or to mitigate that harm; (f) a description of the steps that the organization has taken or intends to take to notify affected individuals ; and (g) the name and contact information of a person who can answer questions about the breach.

## Timing for Reporting

As soon as feasible after the organization determines that the breach has occurred.

## Reporting Obligation (Y/N)

Yes,

## Threshold for Breach Reporting

If it is reasonable in the circumstances to believe that the breach creates a real risk of significant harm to an individual. "Significant harm" includes (without limitation) 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. The sensitivity of the information and the probability of misuse are both relevant to determining whether a breach gives rise to a real risk of significant harm.

## Communication to Data Subjects


Yes, the organization must notify impacted individuals. The notification must contain sufficient information to allow the individual to understand the significance to them of the breach and to take steps, if any are possible, to reduce the risk of harm that could result from it or to mitigate that harm, including: (a) a description of the circumstances of the breach; (b) the day on which, or period during which, the breach occurred or, if neither is known, the approximate period; (c) a description of the personal information that is the subject of the breach to the extent known; (d) a description of the steps that the organization has taken to reduce the risk of harm that could result from the breach;

[Back to countries](#) 

# Lyndsay A. Wasser

 Canada

 lyndsay.wasser@mcmillan.ca

 +1 416.865.7083

 mcmillan.ca



(e) a description of the steps that affected individuals could take to reduce or mitigate the risk of harm; and (f) contact information that the affected individual can use to obtain further information. The notice must generally be provided directly to the individual by telephone, mail, email or any other form of communication that a reasonable person would consider appropriate in the circumstances. However, indirect notification must be given if: (a) direct notification would be likely to cause further harm to the affected individual; (b) direct notification would be likely to cause undue hardship for the organization; or (c) the organization does not have contact information for the affected individual. Indirect notification must be given by public communication or similar measure that could reasonably be expected to reach the affected individuals.

## Other Notification Obligations

Organizations must also notify any other organization and/or government institution (or part of a government institution), if the notifying organization believes that the other organization or the government institution (or part thereof) may be able to reduce or mitigate the risk of harm

## Additional Notes

(1) PIPEDA is Federal legislation that only applies to "personal information" that: (a) an organization collects, uses or discloses in the course of international or interprovincial commercial activities, and commercial activities within provinces that have not enacted substantially similar legislation; and/or (b) is about an employee of, or an

applicant for employment with, the organization, and which the organization collects, uses or discloses in connection with the operation of a federal work, undertaking or business.

(2) Under PIPEDA, organizations must also maintain a record of every breach of security safeguards (regardless of whether the breach gives rise to any risk of harm) for 24 months after the day on which the organization determines that the breach has occurred.

(3) A number of provinces have also enacted privacy and data protection statutes that may be applicable to the private sector, the public sector, and/or the health sector within such provinces. Some of the provincial statutes also include breach reporting and notification obligations.

(4) Certain industries are also subject to specific reporting obligations. For example, without limitation, federally regulated financial institutions (FRFI) are required to report a technology or cyber security incident that has the potential to, or has been assessed to, materially impact the normal operations of a FRFI (including the confidentiality, integrity or availability of its systems and information) to the Office of the Superintendent of Financial Institutions Canada within 24 hours (or sooner, if possible).


(5) Given the complexity of breach reporting requirements in Canada, local counsel should be consulted in every case to determine what federal, provincial, and/or sector-specific reporting and notification obligations apply in the circumstances.

[Back to countries](#) 

# Richard Ma

 China

 richard.ma@dahuilawyers.com

 +86 10 6535 5888

 www.dahuilawyers.com



## Legislation

Personal Information Protection Law

## Type(s) of Breach(es)

Where personal information has been or may be divulged, tampered with or lost, the personal information processor shall immediately take remedial measures and notify the authorities performing duties of personal information protection and the individuals concerned.

Where the personal information processor has taken measures to effectively avoid harm caused by divulgence, tampering with or loss of information, the personal information processor may opt not to notify the individuals concerned; if the authorities performing duties of personal information protection believe that harm may be caused, they may require the personal information processor to notify the individuals concerned.

## Notification to Regulator(s)

Yes. The report must include:

- (I) the types, reasons and possible harm of the information that has been involved or may be involved in the divulgence, tampering with or loss of personal information;
- (II) the remedial measures taken by the personal information processor and the measures that can be taken by the individuals to mitigate harm; and
- (III) the contact information of the personal information processor.

## Timing for Reporting

Where personal information has been or may be divulged, tampered with or lost, the personal information processor shall immediately take remedial measures and notify the authorities performing duties of personal information protection and the individuals concerned.

There will be supplementary regulations for specifying the period.

## Reporting Obligation (Y/N)

Yes

## Threshold for Breach Reporting

Where personal information has been or may be divulged, tampered with or lost

## Communication to Data Subjects

- (I) the types, reasons and possible harm of the information that has been involved or may be involved in the divulgence, tampering with or loss of personal information;
- (II) the remedial measures taken by the personal information processor and the measures that can be taken by the individuals to mitigate harm; and
- (III) the contact information of the personal information processor.

## Other Notification Obligations

N/A

## Additional Notes

N/A


[Back to countries](#) 



# Andrea Garzon

 Colombia

 agarzon@vanegasmorales.com

 +57 3213136912

 vanegasmorales.com



## Legislation

Law 1581 of 2012 - Circular Única SIC

## Type(s) of Breach(es)

A data breach occurs when any of the following characteristics are compromised in the database: confidentiality, integrity, or availability.

These situations can occur for a various reasons, such as the absence of policies or measures to protect the information, human mistakes or negligence, unforeseeable circumstances, cybercrimes, faulty procedures, deficiencies in the company's operations, and the modification, destruction, theft, or loss of the information.

This is just an exemplary list and is not an exhaustive list of data breaches.

## Notification to Regulator(s)

Yes, the organization must report the breach to the Data Protection Authority (DPA). The report must include:

- The organization's name and contact details
- The types or nature of information involved
- The type of breach
- The date of the event and the date the competent area was informed
- The cause of the breach
- A description of the data breach
- The number of data subjects affected by the breach

[Back to countries](#) 

The report must be submitted to the National Registry of Databases (in Spanish, Registro Nacional de Bases de Datos, RNBD) if the company has assets exceeding 100,000 Tax Value Unit. If the company does not meet this criterion, the report must be sent by email to [contactenos@sic.gov.co](mailto:contactenos@sic.gov.co).

## Timing for Reporting

Companies have 15 working days from the moment they detect a data breach and notify the competent area to report the breach to the authority

## Reporting Obligation (Y/N)

Yes

## Threshold for Breach Reporting

According to literal n of article 17 and literal k of article 18 of Law 1581 of 2012, controllers and processors must inform the Data Protection Authority (DPA) of any security code violations or risks in the administration of information.

According to Chapter II, Title V of the "Circular Unica SIC," companies have 15 working days from the moment they detect a data breach and notify the competent area to report the breach to the authority. Regardless of the size or complexity of the breach, every data breach must be reported.


After notifying the DPA, the company must inform the data subjects of the situation in order to let them take actions to protect themselves from the breach.

[https://www.sic.gov.co/sites/default/files/files/Publicaciones/Guia\\_gestion\\_incidentes\\_dic21\\_2020.pdf](https://www.sic.gov.co/sites/default/files/files/Publicaciones/Guia_gestion_incidentes_dic21_2020.pdf)

# Andrea Garzon

 Colombia

 agarzon@vanegasmorales.com

 +57 3213136912

 vanegasmorales.com



## Communication to Data Subjects

The first step is to contain the breach and take remedial action. Next, the company must evaluate the risks and impacts of the data breach and identify the damages to data subjects, companies, or the general public. After that, the company has to inform the Data Protection Authority (DPA) of the breach and notify the data subjects. Finally, the company must learn from its mistakes and take steps to prevent future data breaches. All of this process must be documented in detail in an internal protocol of the company.

## Other Notification Obligations

N/A

## Additional Notes


N/A

[Back to countries](#) 

# Erika Leinonen

 Finland

 erika.leinonen@lexia.fi

 +358 45 7820 0310

 www.lexia.fi

**LEXIA**  
Legal Excellence



## Legislation

GDPR, Finnish Data Protection Act, Finnish Act on the Protection of Privacy in Working Life and Act on Electronic Communications Services. In addition, there are also reporting obligations in special legislation for sector specific supervisory authorities.

## Type(s) of Breach(es)

As defined in GDPR: a personal data breach occurs when 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.

A "personal data" means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

## Notification to Regulator(s)

Yes. Personal data breaches must be reported to the Office of the Data Protection Ombudsman without undue delay and, where feasible, not later than 72 hours after the controller has become aware of the personal data breach.

The Office of the Data Protection Ombudsman's data breach notification form contains three notification types: Complete notification, Preliminary notification and

Complementary notification.

A complete notification is filed if the controller is aware of the details of the data breach. Some details may still be unclear when filing the notification, but it is clear to the controller based on the facts uncovered that the incident involves a personal data breach that meets the criteria for notifying the supervisory authority.

The preliminary notification is intended to give controllers the opportunity to report observations of potential personal data breaches when the details are still scarce or unclear. If a controller files a preliminary notification, it must complement the notification on its own initiative when it obtains more information about the incident. Sector specific reporting requirements are defined in special legislation but the requirements are more or less in line with the GDPR obligations. Data breach notification can be found [here](#)

## Timing for Reporting

Personal data breaches must be reported to the Office of the Data Protection Ombudsman without undue delay and, where feasible, not later than 72 hours after the controller has become aware of the personal data breach.

The controller shall then communicate the personal data breach to the data subject without undue delay.

## Reporting Obligation (Y/N)

yes, in certain cases


[Back to countries](#) 



# Erika Leinonen

 Finland

 erika.leinonen@lexia.fi

 +358 45 7820 0310

 www.lexia.fi

**LEXIA**  
Legal Excellence

## Threshold for Breach Reporting

If a personal data breach can cause a risk to the rights and freedoms of natural persons, the supervisory authority must be notified. In Finland, the Office of the Data Protection Ombudsman functions as the supervisory authority.

Data subjects must be notified of personal data breaches if they are likely to cause a high risk to their rights and freedoms. The controller shall then communicate the personal data breach to the data subject without undue delay, so that the data subject can take measures such as blocking their credit cards.

## Communication to Data Subjects

Data subjects must be notified of personal data breaches if they are likely to cause a high risk to their rights and freedoms. The controller shall then communicate the personal data breach to the data subject without undue delay.

The organisation should provide the following information in the communication:

- a description of the nature of the personal data breach
- the name and contact details of the data protection officer or other contact point where more information can be obtained
- the likely consequences of the personal data breach and
- measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

The communication will not be required if:

**Back to countries** 

- the controller has implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach (in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption)

- the controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects is no longer likely to materialise or

- it would involve disproportionate effort, for example, if it is not known who the affected data subjects are. The matter shall be assessed in light of the risks. If the data subjects cannot be contacted personally, a public communication or similar measure whereby the data subjects are informed in an equally effective manner must be used.

If the controller has not already communicated the personal data breach to the data subject, the supervisory authority may require it to do so.

## Other Notification Obligations

Electronic communication providers and Fi-domain registrars have a notification obligation to NCSC-FI according to Act on Electronic Communications Services. Notification can be made [here](#)

## Additional Notes

Examples of personal data breaches include:

- lost data transfer devices, such as USB memory sticks
- stolen computers
- hacking
- malware infection
- cyber attacks
- fire in the data centre and
- mailing a bank statement to the wrong person

# Jean-Christophe Chevallier

France

jc.chevallier@ydes.com

01 70 92 95 95

www.ydes.com



## Legislation

Act N°78-17 of 6 January 1978 on Information Technology, Data Files And Civil Liberties

## Type(s) of Breach(es)

An eligible data breach occurs when the following criteria are met:

- Controller and/or processor implemented a processing of personal data
- These personal data has been subject to a breach (proven or not proven loss of availability, integrity or confidentiality, whether accidental or unlawful)

## Notification to Regulator(s)

Yes. The organisation shall report the data breach to the CNIL.

The report shall include:

- the organisation's name and contact details;
- the nature of the data breach;
- the date and hour of the beginning of the data breach and the date and hour of the end of the data breach;
- if possible, the categories and approximate number of data subjects affected by the data breach;
- the categories and approximate number of personal data records affected
- the likely consequences of the data breach;
- the steps the organisation has taken or plan to take to prevent a recurrence of the data breach or to mitigate any negative consequences.

## Timing for Reporting

The notification must be sent to the CNIL as soon as possible following the discovery of a eligible data breach .

If organisation are unable to provide all the information required within this timeframe because further investigations are necessary, they may proceed with a notification in two stages:

An initial notification within 72 hours, if possible, following the discovery of the violation;

If the 72-hour deadline is exceeded, organisations shall explain the reasons for the delay in their notification;

Finally, a complementary notification as soon as additional information is available

There is no timeframe for the notification of the data subjects but we can imagine that a "prompt notification" are awaited by the CNIL.

## Reporting Obligation (Y/N)

yes, in certain cases

## Threshold for Breach Reporting

When the organisation has reasonable grounds to believe an eligible data breach has occurred, and the data breach constitutes a risk to the privacy of the data subjects, the organisation shall promptly (within 72 hours) notify the French Data Authority (CNIL).


If there is a high risk regarding privacy of the data subjects the organisation shall also notify them.

[Back to countries](#) >

# Jean-Christophe Chevallier

 France

 jc.chevallier@ydes.com

 01 70 92 95 95

 www.ydes.com

**YDES**

## Communication to Data Subjects

At a minimum, the notification to data subjects shall contain and set forth, in clear and specific terms, the following:

- (i) the nature of the data breach ;
- (ii) the likely consequences of the data breach;
- (iii) the contact details of the person to be contacted (DPO or other);
- (iv) the measures taken to remedy the data breach and, if necessary, to limit the negative consequences of the breach.

The notification must be supplemented, where necessary, with recommendations to data subjects to mitigate the potential negative effects of the violation and to enable them to take the necessary precautions.

There is no obligations regarding how to notify data subjects but the CNIL can control it to be sure of the effectiveness of the notification.

## Other Notification Obligations

N/A


[Back to countries](#) 



# Pàdraig Walsh

 Hong Kong

 padraigwalsh@tannerdewitt.com

 +852 2573 5000

 www.tannerdewitt.com



## Legislation

Personal Data (Privacy) Ordinance (Cap. 486) ("PDPO")

## Type(s) of Breach(es)

A data breach is generally taken to be a suspected breach of data security of personal data held by a "data user", by exposing the data to the risk of unauthorised or accidental access, processing, erasure, loss or use.

## Notification to Regulator(s)

There is no statutory requirement to notify a data breach to the PCPD, but it is encouraged as best practice. Notification should be made to the PCPD's office. Depending on the circumstances of the breach, a notification may include: (a) a general description of the breach; (b) the date, time and duration of the breach; (c) when the breach was discovered; (d) the source of the breach; (e) a list of the types of personal data involved; (f) an assessment of the risk of harm as a result of the breach; (g) a description of the measures taken to date to prevent further loss, unauthorised access etc; (h) the contact information of relevant individuals making the notification/who can be contacted for follow-up information; (i) information on what data subjects can do to protect themselves in light of the breach; and (j) who else has been notified. Care should be taken in determining what information is included in the notification so as not to compromised any ongoing investigations.

For notifications to other authorities, please see the "Additional Notes" box.

## Timing for Reporting

As soon as practicable after the detection of the breach, except where law enforcement agencies have requested a delay due to ongoing investigations.

## Reporting Obligation (Y/N)

Generally no, although the Privacy Commissioner for Personal Data ("PCPD") has stated that its recommended best practice is to make a notification.

## Threshold for Breach Reporting

The person notifying should consider whether a real risk of harm is reasonably foreseeable as a result of the data breach. The consequences of failing to notify should be considered, as should the circumstances of the data breach.

## Communication to Data Subjects

There is no statutory requirement to notify a data breach to impacted individuals, but it is encouraged as best practice where there is a real risk of harm. The notification must contain sufficient information to allow affected data subjects to decide what they need to do to protect themselves from further harm.

## Other Notification Obligations


Notification requirements apply in certain regulated sectors, such as financial services. Contractual notification obligations may arise according to the contractual terms of the data user suffering the data breach. Depending on the circumstances, a report to law enforcement agencies may be warranted, though not mandatory.

[Back to countries](#) 

# Pàdraig Walsh

 Hong Kong

 padraigwalsh@tannerdewitt.com

 +852 2573 5000

 www.tannerdewitt.com



## Additional Notes

The PCPD has recently proposed reforms to the PDPO, which would result in **changes to the data breach reporting requirements in Hong Kong**. A personal data breach will be defined to mean 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. The notification threshold is proposed to be that there is a real risk of significant harm. The notification must be made to the PCPD and the affected data subjects. Notification will have to occur as soon as practicable but not more than five business days after the data user becomes aware of the personal data breach. The notification to the PCPD will be a written notification by way of email, fax or post. Information to be included in the notification and include: (a) a description of the data security incident; (b) the cause of the personal data breach; (c) the types and amount of personal data involved; (d) an assessment of the risk of harm; (e) remedial action taken by the data user to mitigate the risk of harm; and (f) action that data subjects should take.

In the **forthcoming cybersecurity law in Hong Kong**, there will be notification obligations in respect of a broader range of information than personal data in certain sectors with critical infrastructure.

[Back to countries](#) 

# Endre Varady



Hungary



varady@vjt-partners.com



+36 1 501 9900



www.vjt-partners.com.



## Legislation

Article 32-34 of the GDPR

## Type(s) of Breach(es)

Personal data breach resulting in accidental or unlawful destruction, loss, alteration, unauthorized disclosure or unauthorized access to personal data transmitted, stored or otherwise processed. In case of organizations falling under GDPR, the security breach must relate to personal data.

## Notification to Regulator(s)

In general, the personal data breach must be notified via the online system of the Data Protection Authority. A very detailed notification form must be filled out online (see the sample notification form in the Hungary folder). Although this could help the controllers to approach the risk assessment better, it also makes meeting the 72-hour notification deadline more difficult (even if the organization makes notifications in phases).

## Timing for Reporting

The general rule is that as soon as feasible after the organization determines that the breach has occurred but no more than 72 hours after getting knowledge about the personal data breach

## Reporting Obligation (Y/N)

Yes

## Threshold for Breach Reporting

The Hungarian Data Protection Authority takes a black-and-white approach whereby anything beyond "not occurred" (i.e. there is an absolute certainty that no adverse effect occurred in the context of personal data) is reportable (for example there is unauthorized access to the database, but the database is encrypted and the encryption key has not been compromised).

## Communication to Data Subjects

Impacted individuals must be notified only if the data breach results in high risks to the rights and freedoms of such individuals (unless an exception rule applies based on Article 34 (3) of the GDPR). In such cases, the personal data breach shall be communicated without undue delay to impacted individuals. In this notification the data controller shall describe in clear and plain language the nature of the personal data breach and contain at least the information and measures referred to in points (b), (c) and (d) of Article 33(3) of the GDPR. Notification is highly recommended if the score of the ENISA methodology ([available here](#)) is above 3.

## Other Notification Obligations

Generally, notification of other entities involved (e.g., data recipients, entities disclosing the data) may be required to prevent the potential impact the security breach may have, as per GDPR rules.


Back to countries



## Endre Varady

 Hungary

 varady@vjt-partners.com

 +36 1 501 9900

 www.vjt-partners.com.



### Additional Notes

Irrespective whether the threshold for notification is reached, organizations must document all relevant information about personal data breaches.

The bottom line is that organizations must do everything in their power to remedy the personal data breach, i.e. mitigate the effects of personal data breaches and correct the processes to prevent future breaches. The Data Protection Authority recommends to take the following steps in the course of data breach management: to have a proper data breach internal policy in place, a dedicated data breach management team, involvement of the senior management and the DPO, forensic analysis, continuous monitoring, documenting, and working out right action plans.

In this table, we presented the general overview of the personal data breach mechanism, but there are also some additional sector-specific notification rules (with some different rules on timing/threshold). For example, this includes the following specialties:

- Electronic communication providers must notify about the personal data breach to the Hungarian Telecom Authority (first notification within 24 hours, second notification within 72 hours after getting knowledge about the breach) if it is expected that the breach will adversely affect the personal data of subscribers or other individuals.

- Organizations falling under the Hungarian implementation of the CER Directive must report incidents without undue delay to the central incident management centre if the incident has the potential to significantly disrupt the provision of the essential service.

- Organizations falling under the Hungarian implementation of NIS2 Directive must report incidents without undue delay to the central incident management centre in specific cases (such as serious disruption or damage to the provision of service or substantial pecuniary or non-pecuniary damage).

[Back to countries](#) 

# Stephen Mathias

India

stephen.mathias@bgl.kochhar.com

+91 80 4030 8000

www.kochhar.com



## Legislation

### Legislation

The Information Technology Act 2000 ("IT Act") and the directions issued by the Indian Computer Emergency Response Team ("CERT-In") under Section 70B of the IT Act ("Directions").

### Type(s) of Breach(es)

Cybersecurity incidents meeting any of the the following criteria are mandatorily required to be reported ("Reportable Cybersecurity Incident"):

- a) incidents of a severe nature on any part of the public information infrastructure including backbone network infrastructure;
- b) data breaches;
- c) data leaks;
- d) large scale or frequent incidents; or
- e) incidents impacting safety of human beings.

"Cybersecurity incident" means any real or suspected adverse event in relation to cyber security that violates an explicitly or implicitly applicable security policy resulting in unauthorised access, denial or disruption of service, unauthorised use of a computer system or changes in data without authorisation. Cybersecurity incidents meeting any of the the following criteria are mandatorily required to be reported ("Reportable Cybersecurity Incident"):

- a) incidents of a severe nature on any part of the public information infrastructure including backbone network infrastructure;
- b) data breaches;
- c) data leaks;
- d) large scale or frequent incidents; or
- e) incidents impacting safety of human beings.

"Cybersecurity incident" means any real or suspected adverse event in relation to cyber security that violates an explicitly or implicitly applicable security policy resulting in unauthorised access, denial or disruption of service, unauthorised use of a computer system or changes in data without authorisation.

### Notification to Regulator(s)

Yes, the organization must report all Reportable Cybersecurity Incidents to the CERT-In. The incident reporting form prescribed by the CERT-In includes the following details:

- the contact information of the reporting entity;
- details of affected entity (if different from the reporting entity);
- the nature of the incident that has occurred;
- basic information regarding the affected system;
- whether the affected system/network is critical to the reporting entity; and
- date and time of the occurrence and detection of the incident.

The incident reporting form prescribed by the CERT-In is [available here](#). However, it is not mandatory to use the said prescribed form to report incidents, and alternatively, the incident can also be reported to the CERT-In in any other readable form. We however recommend use of the prescribed form.

### Timing for Reporting


An organization must notify the CERT-In of any reportable cybersecurity incident within 6 hours of noticing such incident. However, the 6-hour rule is generally not complied with, and are not aware of any instance wherein the same has been enforced.

Back to countries >

# Stephen Mathias

 India

 stephen.mathias@bgl.kochhar.com

 +91 80 4030 8000

 www.kochhar.com



## Legislation

### Reporting Obligation (Y/N)

Yes

### Threshold for Breach Reporting

When an organization notices that a Reportable Cybersecurity Incident has occurred, it has to notify the CERT-In of such incident.

### Communication to Data Subjects

The Directions do not contain any requirement to notify impacted individuals.

However, do note that under India's new privacy law, the Digital Personal Data Protection Act, 2023 ("DPDPA"), a data controller has to report all personal data breaches to the Data Protection Board of India (to be constituted under the DPDPA) and the affected data subject. The DPDPA has however not come into force as yet and the Indian government is expected to implement the DPDPA in second half of 2024.

### Other Notification Obligations

N/A

### Additional Notes

Please note that in addition to the Directions, there are breach reporting requirements under sector specific cybersecurity regulations that apply to regulated entities in the banking, payments, securities, and insurance sectors. Such regulated entities will have to comply with the Directions and the applicable sector specific regulation.

The "Digital Personal Data Protection Act 2023" which is yet to come into force also prescribes data breach notifications to the data protection authority and to data subjects. However, the law is not yet in force and exact requirements will be firmed up through the rules, drafts of which are yet to be issued

[Back to countries](#) 



## Chiara Agostini



## Luca Egitto



### Legislation

Regulation (EU) 2016/679 - General Data Protection Regulation (GDPR), and Legislative Decree 196/2003 as amended by Legislative Decree 101/2018

### Type(s) of Breach(es)

Accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed. This may include, for example, loss of control over personal data, limitation of certain rights, identity theft or risk of fraud, loss of confidentiality of personal data protected by professional secrecy, financial loss, damage to reputation and any other significant economic or social disadvantage.

### Notification to Regulator(s)

Yes. The data controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of the data breach, notify it to the Italian Data Protection Authority. The notification shall at least:

- (a) describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;
- (b) communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;
- (c) describe the likely consequences of the personal data breach;

(d) describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects. Within the website of the Italian Data Protection Authority is published a model of notification of a personal data breach available at this link <https://www.garanteprivacy.it/documents/10160/0/Modello+notifica+Data+Breach.pdf/6d1fa433-88dc-2711-22ab-dd5d476abe74?version=2.0>

### Timing for Reporting

Not later than 72 hours after having become aware of the data breach

### Reporting Obligation (Y/N)

yes

### Threshold for Breach Reporting

The data controller has to notify the data breach to the Italian Data Protection Authority unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons.

### Communication to Data Subjects

The data controller has to communicate the data breach to the data subjects involved, without undue delay, whether the data breach is likely to result in a high risk to their rights and freedoms. The communication shall outline in clear and plain language: a) a description of the nature of the breach; b) the name and contact details of the data protection officer or other contact point; c) a description of the likely consequences of the breach; and d) a description of the measures

Back to countries >

# Luca Egitto



Italy



luca.egitto@rplt.it



+39 02 87313335



www.rplt.it



taken or proposed to be taken by the controller to solve the breach. Article 34 par. 3 of GDPR states three conditions that, if met, do not require notification to individuals in the event of a breach. These are: 1) the controller has implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption; 2) the controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects is no longer likely to materialise; 3) it would involve disproportionate effort. In such a case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner. In any case, the supervisory authority, having considered the likelihood of the personal data breach resulting in a high risk, may require the data controller to notify the data breach to the data subjects involved.

## Other Notification Obligations

N/A

## Additional Notes

1. Definitions and general information: GDPR is a European Regulation that imposes obligations onto data controller located anywhere, so long as they target or collect data related to people in the EU. According to GDPR, data controller is the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data. Moreover, the Regulation applies only with reference to

the processing of personal data defined as any information relating to an identified or identifiable natural person.


2. Additional requirements in case of data breach: if the data controller has appointed a Data Protection Officer (DPO), as required by article 37, the DPO should play an important role in assisting the controller during the procedure of notification. In this light, it is recommended to promptly inform the DPO about the existence of a breach and to involve him throughout the breach management and notification process. Moreover, according to GDPR, in case of data breach, in addition to the requirements set out before, the data controller shall document the violation in a dedicated record, filling it with the facts relating to the breach, its effects and the remedial action taken, in order to enable the supervisory authority to verify, in any moment, his compliance with GDPR provisions.

[Back to countries](#) >

# Akira Matsuda

 Japan

 amatsuda@iwatagodo.com

 +81 332146205

 www.iwatagodo.com



## Legislation

The Act of Protection of Personal Information ("APPI")

## Type(s) of Breach(es)

A Reportable Incident is any of the following Data Breach Incident:

- a) Data Breach Incident concerning Sensitive Personal Information;
- b) Data Breach Incident with a material risk of resulting in property damage by unauthorized use thereof;
- c) Data Breach Incident resulting from actions taken against the organisation which may have been conducted for fraudulent purposes; or
- d) Data Breach Incident with a reasonable likelihood of the number of data subjects exceeding 1,000 persons.

- "Data Breach Incident" means a leakage or destruction of, or damage to, Personal Data (excluding data which is encrypted with advanced techniques or other measures necessary to protect the rights and interests of individuals) which is or a likelihood that such an incident has occurred.

- "Personal Data" means Personal Information that constitutes a personal information database or other collection of information organized in a systematic way in accordance with the APPI.

- "Personal Information" means means information relating to a living individual which contains: (i) name, date of birth, or other identifier or the equivalent (excluding individual identification codes) which can be used to identify a specific individual (this includes any information that can be easily collated with other information and thereby used to identify that specific individual); or (ii) an individual identification code.

[Back to countries](#) 

## Notification to Regulator(s)

yes. The organisation must report to the PPC. The report must include:

- the organisation's name and contact details;
- a description of the Reportable Incident;
- the items of Personal Information involved;
- number of data subjects affected;
- cause(s) of the Reportable Incident;
- secondary damage or the possibility of secondary damage and its details;
- measures taken in relation to the data subjects affected (including notification);
- whether the organisation has made any public announcement of the Reportable Incident;
- measures to prevent recurrence of a Data Breach Incident; and
- other matters of reference.

## Timing for Reporting

after becoming aware of the Reportable Incident or the threat thereof. It is sufficient for the preliminary report to include only the items the organisation has been able to discover at the timing of making the report.

The affected organisation must submit a final report to the PPC within 30 days (60 days in case of Reportable Incident (c)) after becoming aware of the Reportable Incident or the threat thereof. The final report generally must include all the items required to be reported.

Affected organisations must promptly notify data subjects. What is considered "promptly" will vary depending on the circumstances.

## Reporting Obligation (Y/N)


yes



# Akira Matsuda

 Japan

 amatsuda@iwatagodo.com

 +81 332146205

 www.iwatagodo.com



## Threshold for Breach Reporting

When the organisation becomes aware of a Reportable Incident or the threat thereof, they must promptly notify the Personal Information Protection Commission ("PPC").

## Communication to Data Subjects

The organisation must notify the data subjects affected of the occurrence of the Reportable Incident, except when notifying the data subjects is difficult, and the necessary alternative measures are taken to protect such data subject's rights and interests. The notification must include:

- a description of the Reportable Incident;
- the items of Personal Information involved;
- cause(s) of the Reportable Incident;
- presence or absence of secondary damage or the possibility of secondary damage and its details; and
- other matters of reference.

Notification is considered to be "difficult" when the organisation does not have data subject's contact details or the contact details are out dated and data subjects are not reachable.

"Alternative measures to protect data subject's rights and interests" include measures such as public announcement of the Reportable Incident, and establishing a hotline for data subjects to contact and check whether their Personal Data has been breached or not.

## Other Notification Obligations

N/A

## Additional Notes

Examples of Data Breach Incidents include:


- loss or theft of physical devices (such as laptops and storage devices) or paper records that contain Personal Data;
- unauthorised access to Personal Data by an employee who then discloses it to a third party;
- inadvertent disclosure of Personal Data due to 'human error', for example an email sent to the wrong person; and
- encryption of Personal Data by a ransomware which is unrecoverable.

[Back to countries](#) 

## Stephan Mulders

 Netherlands

 s.mulders@vandiepen.com


 +316 23 57 96 62

 www.vandiepen.com



## Bartosz Sujecki

 b.sujecki@vandiepen.com

 +3120 - 574 74 74



### Legislation

N/A

### Type(s) of Breach(es)

An eligible data breach occurs when the following criteria are met:

a) There is unauthorised access to, or disclosure of, personal information held by an organisation, or information is lost in circumstances where unauthorised access or disclosure is likely to occur;

b) This is likely to result in serious harm to any of the individuals to whom the information relates; and

c) The organisation has been unable to mitigate the serious harm occurring.

"Personal Information" means information or an opinion about an individual who is identified, or reasonably identifiable.

"Serious harm" will depend on the kind / sensitivity of the information, "who" has obtained the information, the type and extent of security measures in place, and the nature of the harm.

### Notification to Regulator(s)

When the organisation has reasonable grounds to believe an eligible data breach has occurred, they must promptly notify any relevant individual at risk of serious harm, and notify the DPA (link and details).

### Timing for Reporting

Organisations subject to the 'Notifiable Data Breach' scheme are required to conduct an assessment of any 'suspected' eligible data breaches and take reasonable steps to

complete this assessment within 30 days.

Affected organisations must notify individuals as soon as practicable after completing the statement prepared for notifying the DPA.

### Reporting Obligation (Y/N)

Yes

### Threshold for Breach Reporting

When the organisation has reasonable grounds to believe an eligible data breach has occurred, they must promptly notify any relevant individual at risk of serious harm, and notify the DPA (link and details).

### Communication to Data Subjects

The first step is to contain the breach where possible and take remedial action. Where serious harm cannot be mitigated through remedial action, the organisation must notify individuals at risk of serious harm (either by notifying all individuals, or only those individuals at risk of serious harm).

If it is not practicable to notify individuals at risk of serious harm, the organisation must publish a copy of the statement prepared for the DPA on its website, and take reasonable steps to bring its contents to the attention of individuals at risk of serious harm.

### Other Notification Obligations

N/A

[Back to countries](#) 

# Stephan Mulders



Netherlands



s.mulders@vandiepen.com



+316 23 57 96 62



www.vandiepen.com



## Additional Notes

Examples of data breaches include:

- loss or theft of physical devices (such as laptops and storage devices) or paper records that contain personal information
- unauthorised access to personal information by an employee
- inadvertent disclosure of personal information due to 'human error', for example an email sent to the wrong person
- disclosure of an individual's personal information to a scammer, as a result of inadequate identity verification procedures.


[Back to countries](#) >



# Alexander Mollan

 Norway

 mollan@braekhus.no

 +47 463 63 277

 www.braekhus.no



## Legislation

Act relating to the processing of personal data of 15 June 2018 no. 38 ("personopplysningsloven" or the "Personal Data Act").

Please note that the Regulation (EU) 2016/679 (the GDPR) is included in the Norwegian Personal Data Act in its entirety.

## Type(s) of Breach(es)

Personal data breach as defined by the GDPR Article 4 no. 12, i.e. 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.

As defined by the GDPR Article 4 no. 1, "personal data" means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

## Notification to Regulator(s)

Yes. Controllers must notify breaches to the Norwegian Data Protection Authority. As defined by the GDPR Article 4 no. 7, a "Controller" is the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.

[Back to countries](#) 

The notification shall at least include: (a) a description of the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned; (b) the name and contact details of the data protection officer or other contact point where more information can be obtained; (c) a description of the likely consequences of the personal data breach; and (d) a description of the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

## Timing for Reporting

The Norwegian Data Protection Authority: As a main rule, a controller must notify the Norwegian Data Protection Authority of the personal data breach without undue delay and no later than 72 hours after the controller became aware of the breach.

If a controller is unable to provide a notification to the supervisory within the deadline, the controller must provide its reasons for this in the delayed notification. The controller may provide the information required in a notification in phases without undue delay, if such information cannot be provided at the same time.


A data processor, i.e. an entity processing personal data on behalf of a controller, must notify the controller without undue delay after becoming aware of a breach. As a minimum, the processor's notification must contain the same information as the notification from the controller to the The Norwegian Data Protection Authority.

Data subjects: Communication must be provided without undue delay.

# Alexander Mollan

 Norway

 mollan@braekhus.no

 +47 463 63 277

 www.braekhus.no



## Reporting Obligation (Y/N)

Yes

## Threshold for Breach Reporting

The Norwegian Data Protection Authority: The controller must report a personal data breach to the authority, unless the breach is unlikely to result in a risk to the rights and freedoms of natural persons.

Data subjects: The controller must communicate a personal data breach to the affected data subject(s), provided that the breach is likely to result in a high risk to the rights and freedoms of natural persons. The controller may refrain from communicating the breach if any of the following conditions are met: (a) the controller has implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption; (b) the controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects is no longer likely to materialise; or (c) it would involve a disproportionate effort. In such a case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner.

## Communication to Data Subjects

As a main rule, controllers must communicate personal data breaches to data subjects. Such communication shall include a description in clear and plain language the

nature of the breach and contain at least the information and measures referred to in points (b), (c) and (d) of the notification requirements to the supervisory authority as described in column F.

## Other Notification Obligations

N/A

## Additional Notes


N/A

[Back to countries](#) 

# Winnie Chang

 Singapore

 winnie.chang@orionw.com

 +65 6909 7801

 www.orionw.com



## Legislation

Personal Data Protection Act 2012  
Personal Data Protection (Notification of Data Breaches) Regulations 2021 ("Regulations")

## Type(s) of Breach(es)

Notifiable data breaches are breaches that:

a) result in, or are likely to result in, significant harm to the affected individuals - the Regulations provide the classes of personal data that are deemed to result in significant harm if they are compromised in a data breach; or

b) are, or are likely to be, of significant scale - these are breaches that involve the personal data of 500 or more individuals.

## Notification to Regulator(s)

Yes. The organisation must report to the Commission, and such a report should include:

- Facts of the data breach (eg. circumstances relating to breach, number of affected individuals etc);
- Data breach handling (an account of the steps taken once the data breach had been discovered); and
- Contact details of at least 1 authorised representative.

## Timing for Reporting

Assessment:  
Once an organisation has credible grounds to believe that a data breach has occurred, the organisation should take reasonable and

expeditious steps to assess if the breach a notifiable data breach within 30 calendar days.

Notification of Commission:

If the organisation assesses that the data breach is notifiable, it must report the breach to the Commission as soon as possible, but in any case no later than 3 calendar days after the assessment was made.

Notification of individual:

where required, affected individuals as soon as practicable, at the same time or after notifying the Commission.

## Reporting Obligation (Y/N)

Yes

## Threshold for Breach Reporting

Assessment:

Where an organisation has reason to believe that a data breach affecting personal data in its possession/under its control has occurred, it must conduct, in a reasonable and expeditious manner, an assessment of whether the data breach is a notifiable data breach.

Where a data intermediary has reason to believe that a data breach has occurred in relation to personal data that it is processing on behalf of another organisation, the data intermediary must immediately notify the other organisation of such breach and the other organisation must conduct an assessment of whether the breach is a notifiable data breach


[Back to countries](#) 



# Winnie Chang

 Singapore

 winnie.chang@orionw.com

 +65 6909 7801

 www.orionw.com

ORION 

## Communication to Data Subjects

The affected individuals must be notified of a notifiable breach unless steps have been taken/can be taken (whether prior to the breach or after it has occurred) such that the breach will not, or is unlikely to, result in significant harm to affected individuals.

A notification to affected individuals should include:

- Facts of the data breach (eg. circumstances relating to breach and the type of personal data affected);
- Management and remediation plan (eg. potential harm that may result, action taken by organisation to mitigate / remedy failure); and
- Contact Details of at least 1 authorised representative.

## Other Notification Obligations

N/A

## Additional Notes

Potential causes of data breaches:


- Malicious activities by external parties (eg. hacking, ransomware, scams)
- Human errors caused by employees (eg. sending personal data to the wrong recipient, loss of data storage devices)
- Computer system weaknesses (eg. bugs or errors in programming code of websites, databases)

[Back to countries](#) 

# Beatriz Rodriguez Gomez

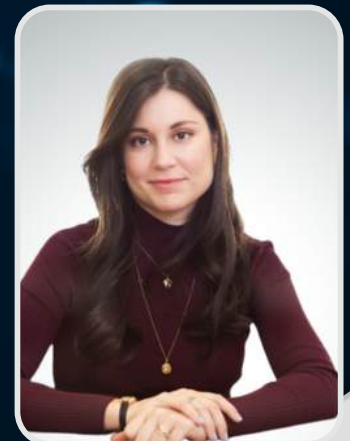
 Spain

 b.rodriuez@rocajunyent.com

 +34.914.41.44.52

 www.rocajunyent.com

RocaJunyent



## Legislation

Organic Law 3/2018, of December 5, on Personal Data Protection and guarantee of digital rights. ("LOPD")

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free

movement of such data, and repealing Directive 95/46/EC ("GDPR")

When the client provides services for public sector, Royal Decree 311/2022, of May 5, on the National Security Framework

When the client has critical infrastructures, Royal Decree 43/2021, January 26, that develops the Royal Law-Decree 12/2018, September 7, on the security of networks and IT systems and that transposed NIS Directive (NIS2 transposition is still pending)

## Type(s) of Breach(es)

'personal data breach' means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;

A notifiable data breach occurs when they are likely to constitute a risk to the rights and freedoms of individuals.

## Notification to Regulator(s)

Notifications of personal data breaches to the AEPD must be made electronically, using the personal data breach notification form in the E-Office, in order to ensure the correct execution of the obligations of Article 33.3 of the GDPR.

## Timing for Reporting

The organisation must notify the notifiable breach to the Spanish Data Protection Agency within 72 hours of the organisation becoming aware of the breach.

## Reporting Obligation (Y/N)

yes

## Threshold for Breach Reporting

When the organisation has become aware that a notifiable data breach has occurred, they must notify without undue delay all individuals whose rights and freedoms may be at risk, and notify the Spanish Data Protection Authority within 72h.

In the public sector, in general, public administrations must report personal data breaches to the Spanish Data Protection Agency, except in the case of the Autonomous Communities of Andalusia, Catalonia, Basque Country, in the case of personal data breaches in public sector entities under their competence, they notify the respective Autonomous Agencies.

## Communication to Data Subjects

The first step is to contain the breach where possible and take remedial action. Where the risk to the rights and freedoms of individuals cannot be mitigated by corrective action, the organisation should notify individuals.


If it is not practicable to notify individuals at risk, the organisation shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner.

Back to countries 

# Beatriz Rodriguez Gomez

 Spain

 b.rodriuez@rocajunyent.com

 +34.914.41.44.52

 www.rocajunyent.com

**RocaJunyent**

## Other Notification Obligations

The notification to the Data Subjects impacted should at least:

- a) indicate the name and contact details of the data protection officer or other contact point where more information can be obtained;
- b) describe the likely consequences of the personal data breach;
- c) describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

## Additional Notes

If there is no obligation to notify the AEPD, it's obligatory to make a report to document the data breach, including the facts related to the breach, its effects and the corrective actions taken.


**Back to countries** 



# John Eastwood

 Taiwan

 john.eastwood@eiger.law

 +886 2 2771 0086

 www.eiger.law



## Legislation

Personal Data Protection Act (PDPA) and its enforcement rules, the Cyber Security Management Act (CSMA) and its regulations.

## Type(s) of Breach(es)

Data breach incidents that involve "critical infrastructure providers" are handled under the CSMA. "Critical infrastructure" is an "asset, system or network, either physical or virtual, once discontinued from operation or becoming less effective, would lead to significant negative impact upon the national security, public interests, living standard of citizens and economic activities." Such data breach incidents are classified into 4 different levels of severity.

All breaches involving personal data fall under PDPA, including those covered by the CSMA. The CSMA may cover breaches that do not involve personal data but any kind of operational technology or data. Organizations subject to the CSMA are designated by the competent authority, while the PDPA generally applies to all organizations.

## Notification to Regulator(s)

Data breaches involving "critical infrastructure" under the CSMA will require a report to their industry-specific competent authority, and in some cases to the Ministry of Digital Affairs (MODA) as well. The report must include:

- the organization's name and contact details
- timing of occurrence or noticing
- a description of the data breach
- evaluation of the level
- remedial steps taken in response to the data breach

- evaluation about whether external support is necessary
- other relevant matters

Breaches not under the CSMA involving personal data will fall under industry-specific requirements for notifications to the government.

## Timing for Reporting

**CSMA:** within 1 hour that the organization learns of the breach, report to the industry-specific competent authority and/or the Ministry of Digital Affairs (MODA).

**PDPA:** within 72 hours after becoming aware of the incident (in general, depending on industry-specific regulations), reporting to the municipal/central competent authority of the industry.

## Reporting Obligation (Y/N)

yes

## Threshold for Breach Reporting

If a breach involves critical infrastructure as defined by the CSMA, then the notification should be within one (1) hour that the organization knows of the breach. If a breach involves personal information, the industry-specific requirements often invoke a "large number" of affected individuals or threats to an organization's ability to operate.

## Communication to Data Subjects

The PDPA and its enforcement rules are flexible in allowing a wide variety of means to notify individuals affected by a breach.

## Other Notification Obligations


N/A

[Back to countries](#) 

# John Eastwood

 Taiwan

 john.eastwood@eiger.law

 +886 2 2771 0086

 www.eiger.law



## Additional Notes

The specific fields considered 'critical' are subject to update from time to time, and have included energy, water, telecommunications, transportation, finance, emergency medical care, government agencies and science parks. There is a formal procedure to have an entity be designated as a critical infrastructure provider. While the list of entities subject to the CSMA is not publicly released, it is understood that not many are currently private entities.

As of 2024, the establishment of the Personal Data Protection Commission (PDPC) is underway, and we do expect that once it is fully up and running there may be some changes in the enforcement environment.

## Contribution

A special thanks to [Nathan Snyder](#), Associate at Eiger Law, and [Sarah Chen](#), Senior Associate, for their valuable contributions to this section on data breach legislation in Taiwan. Their expertise and insights have been instrumental in shaping a comprehensive and accurate understanding of the regulatory landscape and practical considerations in this area.

[Back to countries](#) 

# Ozan Karaduman

Türkiye

ozan@karadumanesin.com

+90 212 995 01 28

www.karadumanesin.com

KARADUMAN & ESİN  
LAW FIRM



## Legislation

Personal Data Protection Law No. 6698 (the "PDPL")

## Type(s) of Breach(es)

The PDPL does not have an explicit definition of a data breach. Article 12(5) of the PDPL sets forth that a notification must be made in case the personal data is obtained unlawfully by third parties, which indicates that the PDPL considers only unauthorized access as data breach. However, the Turkish Data Protection Authority (the "KVKK") has a broader interpretation; the KVKK considers also the cases where the integrity of personal data is compromised or where the data is not accessible to the data controller (e.g. DDoS attacks or ransomware) as data breaches in the Personal Data Breach Notification Form ([provided on the Turkish DPA's website](#)).

## Notification to Regulator(s)

Yes, the breach notification must be reported to the KVKK by filing an online application form. The form must include, inter alia:

- Data controller's name and contact details including the address,
- Time and date of the beginning of the breach
- Time and date of the ending of the breach
- Time and date of the identification of the breach
- Details regarding data processor if it is involved in the breach
- How the breach has occurred and was identified
- Impact of the breach such as security of data, access to data and data integrity
- Categories of personal data that were impacted

- Number of the impacted data subjects
- Groups of data subjects who were impacted from data breach such as patients, customers, children and students
- Impacts of data breach to data subjects such as identity theft, fraud, financial loss, discrimination and to the organization
- Information regarding notification made to data subjects such as the date and notification methods
- Information regarding notification to other institutions or organizations
- Scope and the content of the technical and administrative precautions in place before the breach and their future planning
- Content and scope of the notifications that have been sent to the data subjects and the relevant DPAs
- Potential consequences of the breach

## Timing for Reporting

Data breaches must be duly notified to the DPA within 72 hours after becoming aware of the breach.

Organisations are also obliged to state their reasoning of any delays if the 72 hours duration of notification cannot be met.

Affected organisations must notify individuals as soon as practicable after completing the statement prepared for notifying the DPA.


## Reporting Obligation (Y/N)

yes


Back to countries >



# Ozan Karaduman

 Türkiye

 ozan@karadumanesin.com

 +90 212 995 01 28

 www.karadumanesin.com

KARADUMAN & ESİN  
LEGAL FIRM

## Threshold for Breach Reporting

There is no threshold for breach notification, i.e. there is no qualified notification procedure under the PDPL. Any data breach must be notified to the affected individuals and the KVKK within 72 hours as of the time the data controller becomes aware of the breach.

## Communication to Data Subjects

Organisation must take required actions after the data breach and notify impacted individuals at risk.

If it is not possible to notify all the impacted individuals at risk, the organisation must publish a copy of the statement indicating the relevant information regard to the breach on its website, and take reasonable steps to bring its contents to the attention of the impacted individuals at risk.

## Other Notification Obligations

N/A

## Additional Notes

Examples of data breaches include:


- loss or theft of physical devices (such as laptops and storage devices) or paper records that contain personal information
- unauthorised access to personal information by an employee
- inadvertent disclosure of personal information due to 'human error', for example an email sent to the wrong person
- disclosure of an individual's personal information to a scammer, as a result of inadequate identity verification procedures.

[Back to countries](#) 

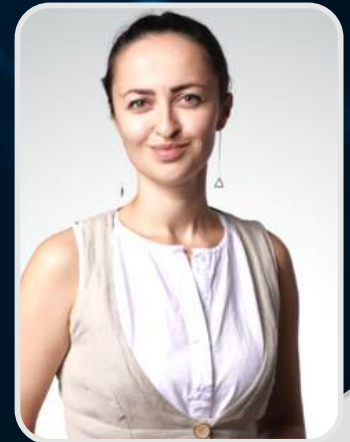
# Oksana Zadniprovska

 Ukraine

 Zadniprovska@axon.partners

 +38 067 672 20 48

 Axon.partners



## Legislation

The Law "On Protection of Information in Information and Communication Systems" of July 5, 1994; Draft Law No. 8153 of October 25, 2022; Resolution of the Cabinet of Ministers of Ukraine No. 373 of March 29, 2006 "Rules for Ensuring Information Protection in Information, Electronic Communication and Information and Communication Systems"

## Type(s) of Breach(es)

A data breach may occur in the event of unauthorized actions with respect to information in the system, which means actions performed in violation of the procedure for access to this information established in accordance with the law.

The Draft Law No. 8153 of October 25, 2022 defines a breach of personal data security as an accidental or unlawful destruction, loss, alteration, unauthorized disclosure of personal data or access to personal data that occurred as a result of a violation of the requirements and conditions for the security of personal data processing;

## Notification to Regulator(s)

The owner of a system that processes state information resources or restricted information must notify a specially authorized central executive body for the organization of special communications and information protection or a subordinate regional body. Such an authorized body in Ukraine is the State Service for Special Communications and Information Protection of Ukraine.

Notification requirements are not defined by Ukrainian legislation.

The Draft Law No. 8153 of October 25, 2022 introduces requirements to notify regulatory authorities of data breach. Such notification must include:

- 1) a description of the nature of the personal data security breach, including the categories and number of personal data subjects affected by the security breach personal data, as well as the categories and number of registration records of personal data affected by the personal data security breach;
- 2) contact details of the responsible person for personal data protection or other person who can provide additional information;
- 3) a description of the likely consequences of the personal data security breach;
- 4) a description of the measures taken or planned by the controller to reduce the the consequences of a personal data security breach.

## Timing for Reporting

The owner of the system used to process information from another system shall notify the owner of the said system of the detected facts of unauthorized actions with respect to the information in the system.

## Reporting Obligation (Y/N)

Yes. But not for every controller (see the "Notification to Regulator(s)" box).


The Draft Law No. 8153 of October 25, 2022 introduces the obligation of the controller to notify the supervisory authority of personal data security breaches.

[Back to countries](#) 

# Oksana Zadniprovska

 Ukraine

 Zadniprovska@axon.partners

 +38 067 672 20 48

 Axon.partners



## Threshold for Breach Reporting

The notification is sent in case of attempts/facts of unauthorized actions in the system regarding state information resources or restricted information, the requirement for protection of which is established by law. Whether this includes all types of personal data or only sensitive categories is still a debatable issue (as it is not clearly established in the law or court practice).

According to the Draft Law No. 8153 of October 25, 2022, the controller must notify the supervisory authority of a breach of personal data security if he or she becomes aware of such a breach, unless the breach of personal data security is unlikely to lead to a risk to the rights and freedoms of an individual.

## Communication to Data Subjects

Given the nature of the information, the law does not require notification of impacted individual(s).

In the event of unauthorized actions in an information and communication system, such actions are subject to mandatory registration in that system.

The Draft Law No. 8153 of October 25, 2022 provides for the obligation of the controller to report security breaches of personal data of the subject of personal data without undue delay if there is a possibility of a high degree of risk to the rights and freedoms of an individual.

## Additional Notes

Ukrainian legislation does not specify a time limit for reporting unauthorized actions in the system.

The Draft Law No. 8153 of October 25, 2022 stipulates that the controller must notify the supervisory authority of a personal data breach immediately, but no later than 72 hours from the moment he or she becomes aware of such a breach.


[Back to countries](#) 



# Kim Walker

 United Kingdom

 kim.walker@shma.co.uk

 +44 (0)207 264 4362

 www.shma.co.uk

 SHAKESPEARE MARTINEAU  
Legal advice for life and business



## Legislation

UK GDPR (having the meaning given to it in section 3(10) (as supplemented by section 205(4)) of the Data Protection Act 2018). See in particular Article 33 UK GDPR. See also the guide on [the ICO website](#) (on which this PR guidance is based)

## Type(s) of Breach(es)

A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data...". This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data. Personal data breaches can include:

- access by an unauthorised third party;
- deliberate or accidental action (or inaction) by a controller or processor;
- sending personal data to an incorrect recipient;
- computing devices containing personal data being lost or stolen;
- alteration of personal data without permission; and
- loss of availability of personal data.

## Notification to Regulator(s)

If a breach is reportable to the ICO it can be reported by phone or (more normally) using the online form on [the ICO website](#). When reporting a breach, the UK GDPR (and the ICO's form) says you must provide: a description of the nature of the personal data breach including, where possible:

- the categories and approximate number of individuals concerned; and

- the categories and approximate number of personal data records concerned;
- the name and contact details of the data protection officer (if your organisation has one) or other contact point where more information can be obtained;
- a description of the likely consequences of the personal data breach; and
- a description of the measures taken, or proposed to be taken, to deal with the personal data breach and, where appropriate, of the measures taken to mitigate any possible adverse effects.

## Timing for Reporting

You must report a notifiable breach to the ICO without undue delay, but not later than 72 hours after becoming aware of it. If you take longer than this, you must give reasons for the delay. The UK GDPR recognises that it will not always be possible to investigate a breach fully within 72 hours to understand exactly what has happened and what needs to be done to mitigate it. So its Article 33(4) allows you to provide the required information in phases, as long as this is done without undue further delay.

## Reporting Obligation (Y/N)

yes

## Threshold for Breach Reporting


When a personal data breach has occurred, you need to establish the likelihood of the risk to people's rights and freedoms. If a risk is likely, you must notify the ICO; if a risk is unlikely, you don't have to report it.

[Back to countries](#) 

# Kim Walker

 United Kingdom

 kim.walker@shma.co.uk

 +44 (0)207 264 4362

 www.shma.co.uk

 SHAKESPEARE MARTINEAU  
Legal advice for life and business

## Communication to Data Subjects

If a breach is likely to result in a high risk to the rights and freedoms of individuals, the UK GDPR says you must inform those concerned directly and without undue delay.

A 'high risk' means the requirement to inform individuals is higher than for notifying the ICO. Again, you will need to assess both the severity of the potential or actual impact on individuals as a result of a breach and the likelihood of this occurring. If the impact of the breach is more severe, the risk is higher; if the likelihood of the consequences is greater, then again the risk is higher. In such cases, you will need to promptly inform those affected, particularly if there is a need to mitigate an immediate risk of damage to them. One of the main reasons for informing individuals is to help them take steps to protect themselves from the effect of a breach.

## Other Notification Obligations

N/A

## Additional Notes

To help you assess whether a breach is reportable to the ICO or not, [the ICO provides examples](#)

Back to countries 

# Gene Price



USA



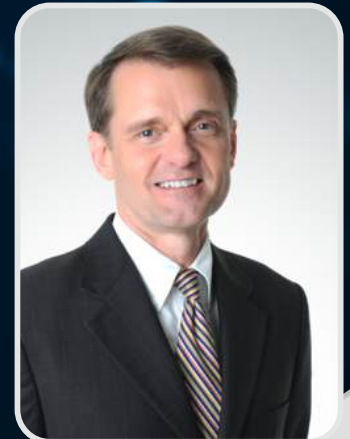
[gprice@fbtlaw.com](mailto:gprice@fbtlaw.com)



502.568.0242



[www.frostbrowntodd.com](http://www.frostbrowntodd.com)



## Legislation

**U.S. Federal Law** - There is no comprehensive data breach notification requirement at the federal level in the U.S. However, there are several statutes and regulations issued by Congress and various federal agencies that mandate data breach reporting and/or notification under specific circumstances, particularly the functional area a company is involved with. The application of these statutes and regulations will depend on the type of data compromised, the type of business, sector, or industry a company or person is in, the class of persons affected by the breach, the number of persons affected, and other factors. Applying these statutes and regulations must be considered on a case-by-case basis, which come from the Federal Trade Commission, the Securities Exchange Commission, the Cybersecurity Infrastructure and Security Agency, among others.

**U.S. State Law** - Each and every state has enacted its own data breach notification law. These laws each apply to their own citizens and/or residents in different ways. Many of these state laws are similar, but applying their requirements must be done on a case-by-case basis. Strictly as a general matter, they often require companies whose data was compromised in one state to consider each person, and their state of residence, domicile, etc., in determining whether notification of a state Attorney General is necessary.

As an example, see the following description of the laws of California that apply in the event of a cyber compromise in that state, or one impacting its citizens.

California has the largest population of any state and tends to regulate technological issues faster than most states within the U.S. It is described here on that basis.

## Type(s) of Breach(es)

A data breach occurs when the following criteria are met regarding a California resident's data:

1) when unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person; or  
 2) when encrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person and the encryption key or security credential was, or is reasonably believed to have been, acquired by an unauthorized person and the person or business that owns or licenses the encrypted information has a reasonable belief that the encryption key or security credential could render that personal information readable or usable.

"Personal information" means:

(1) An individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted:

(A) Social security number.

(B) Driver's license number, California identification card number, tax identification number, passport number, military identification number, or other unique identification number issued on a government document commonly used to verify the identity of a specific individual.

(C) Account number or 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.

(D) Medical information.

(E) Health insurance information.


[Back to countries](#) >



# Gene Price

 USA

 gprice@fbtlaw.com

 502.568.0242

 www.frostbrowntodd.com



(F) Unique biometric data generated from measurements or technical analysis of human body characteristics, such as a fingerprint, retina, or iris image, used to authenticate a specific individual. Unique biometric data does not include a physical or digital photograph, unless used or stored for facial recognition purposes.

(G) Information or data collected through the use or operation of an automated license plate recognition system.

(H) Genetic data.

(2) A username or email address, in combination with a password or security question and answer that would permit access to an online account.

## Notification to Regulator(s)

If the security breach involved more than 500 California residents as a result of the single breach of a security system, a sample copy of the security breach notification must be submitted to the Attorney General of California.

"Breach of the security of the system" means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the person or business.

## Timing for Reporting

For Impacted Individuals, the most expedient time possible and without unreasonable delay. Notification may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation.

## Reporting Obligation (Y/N)

yes

## Threshold for Breach Reporting

When unencrypted personal information or combination of encrypted information and its key or security credentials was acquired by an unauthorized person, OR it is reasonably believed to have been acquired by an unauthorized person.

## Communication to Data Subjects

The notification must be titled "Notice of Data Breach," with the headings: "What Happened", "What Information Was Involved", "What We Are Doing", "What You Can Do", and "For More Information".

The breach notification shall contain:


- The name and contact information of the reporting person or business.
- A list of the types of personal information that were or are reasonably believed to have been the subject of a breach.
- If the information is possible to determine at the time the notice is provided, then any of the following: (i) the date of the breach, (ii) the estimated date of the breach, or (iii) the date range within which the breach occurred.
- The date of the notification.
- Whether notification was delayed as a result of a law enforcement investigation, if that information is available.
- A general description of the breach incident, if that information is possible to determine at the time the notice is provided.

[Back to countries](#) 

# Gene Price

 USA

 gprice@fbtlaw.com

 502.568.0242

 www.frostbrowntodd.com



- The toll-free telephone numbers and addresses of the major credit reporting agencies if the breach exposed a social security number or a driver's license or California identification card number.
- If the person or business providing the notification was the source of the breach, an offer to provide appropriate identity theft prevention and mitigation services must be provided at no cost to affected persons for not less than 12 months.

## Other Notification Obligations

Notification requirements:

- The text of the notification cannot be smaller than 10-point font.

Security breach notification may include:

(A) Information about what the person or business has done to protect individuals whose information has been breached.

(B) Advice on steps that people whose information has been breached may take to protect themselves.

(C) In breaches involving biometric data, instructions on how to notify other entities that used the same type of biometric data as an authenticator to no longer rely on data for authentication purposes.

"notice" may be provided by one of the following methods:

- (1) Written notice.
- (2) Electronic notice, if consistent with e-sign signatures.
- (3) Substitute notice, if the person or business demonstrates that the cost of providing notice would exceed two hundred fifty thousand dollars (\$250,000), or that the affected class of subject persons to be notified exceeds 500,000, or the person or business does not have sufficient contact information. Substitute notice shall consist of all of the following:

(A) Email notice when the person or business has an email address for the subject persons.  
 (B) Conspicuous posting, for a minimum of 30 days, of the notice on the internet website page of the person or business, if the person or business maintains one. For purposes of this subparagraph, conspicuous posting on the person's or business's internet website means providing a link to the notice on the home page or first significant page after entering the internet website that is in larger type than the surrounding text, or in contrasting type, font, or color to the surrounding text of the same size, or set off from the surrounding text of the same size by symbols or other marks that call attention to the link.

(C) Notification to major statewide media.

**NOTE:** for data breaches involving clinics, health facilities, home health agencies, and hospices, California Health and Safety Code provides additional rules. Cal. Civ. Code § 1280.15.

## Additional Notes

No.

[Back to countries](#) 

# CONTACT US

PrivacyRules

**American Headquarters:**

PrivacyRules, Ltd.

151 West 4th Street

Suite 200

Cincinnati, OH 45202, USA

**Email**

info@privacyrules.com

[www.privacyrules.com](http://www.privacyrules.com)

[Contact us for a quotation](#)

