Comparing privacy laws:

GDPR v. Thai Personal Data Protection Act

OneTrust DataGuidance™
REGULATORY RESEARCH SOFTWARE

About the authors

OneTrust DataGuidance™ provides a suite of privacy solutions designed to help organisations monitor regulatory developments, mitigate risk and achieve global compliance.

OneTrust DataGuidance™ Regulatory Research includes focused guidance around core topics (i.e. GDPR, data transfers, breach notification, among others), Cross-Border Charts which allow you to compare regulations across multiple jurisdictions at a glance, a daily customised news service and expert analysis.

These tools, along with our in-house analyst service to help with your specific research questions, provide a cost-effective and efficient solution to design and support your privacy programme.

Blumenthal Richter & Sumet is a full-service independent law firm in Bangkok that helps leading international and domestic companies to expand into new markets, grow their businesses and navigate increasingly complex regulatory frameworks in Thailand and Southeast Asia. For more than 40 years, they have built a reputation for providing international standards of legal service, harnessing insightful local knowledge and operating to the highest degree of integrity at all times.

Contributors

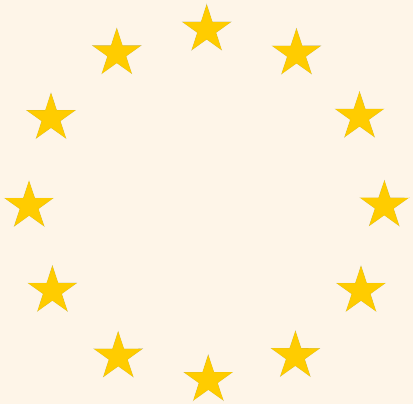
OneTrust DataGuidance™: Alexis Kateifides, Angela Potter, Holly Highams, Angus Young, Tooba Kazmi, Christopher Campbell, Victoria Ashcroft, Keshawna Campbell, Kotryna Kerpauskaite, Emily Dampster, Andrew Filis

Blumenthal Richter & Sumet: John P. Formichella, Naytiwut Jamallsawat, Bruce McNair, Artima Brikshasri

Image production credits:

Cover/p.5/p.55: flowgraph / Essentials collection / istockphoto.com | MicroStockHub / Signature collection / istockphoto.com
Scale key p6-49: enisaksoy / Signature collection / istockphoto.com

Table of contents



Introduction

On 25 May 2018, the General Data Protection Regulation (Regulation (EU) 2016/679) ('GDPR') went into effect. The Personal Data Protection Act, B.E. 2562 (2019) ('PDPA') which is Thailand's first consolidated data protection law, was published in the Thai Government Gazette on 27 May 2019 and will take effect on 27 May 2020.

Both laws aim to guarantee protection for individuals and their personal data, and impose similar obligations on businesses when collecting, using, and disclosing personal data. Additionally, once the data protection authority i.e. the Personal Data Protection Committee ('PDPC') is established, further sub-regulations and guidance on the PDPA will be issued.

The PDPA is largely based on the GDPR, and therefore, there are several similarities between the two. For example, both texts have similar provisions regarding the legal basis of processing, as both list consent, performance of a contract, legal obligations, legitimate interests, or vital interests as a legal basis.

In addition, the PDPA mirrors the GDPR's extraterritorial applicability and applies to data controllers and data processors outside of Thailand if they process personal data of data subjects in Thailand and offer goods and services to, or monitor behaviour of the data subjects. Moreover, both texts empower data subjects with several rights, including the right to erasure, the right to be informed, the right to object, the right to data portability, and the right to access.

Nevertheless, there are some key differences between the PDPA and the GDPR. In particular, unlike the GDPR, the PDPA does not apply to certain public authorities, and the definition of 'personal data' in the GDPR is much more detailed, as it specifically includes IP addresses and cookie identifiers, whilst there is no mention of these in the PDPA. Furthermore, although the PDPA states that a data subject has the right to anonymise their personal data, unlike the GDPR, the PDPA does not define anonymised or pseudonymised data.

Other examples of divergences can be found in the provisions relating to cross-border data transfers, and penalties. Whilst both the GDPR and the PDPA provide for monetary and administrative penalties in case of non-compliance, violations of the PDPA could also result in imprisonment for a term not exceeding one year.

This guide is aimed at highlighting the similarities and differences between these two landmark pieces of legislation in order to assist organisations in complying with both.

Structure and overview of the Guide

This Guide provides a comparison of the two pieces of legislation on the following key provisions:

1. Scope
2. Key definitions
3. Legal basis
4. Controller and processor obligations
5. Individuals' rights
6. Enforcement

Each topic includes relevant articles and sections from the two laws, a summary of the comparison, and a detailed analysis of the similarities and differences between the GDPR and the PDPA.

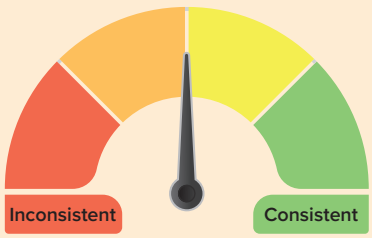
Key for giving the consistency rate

Consistent: The GDPR and the PDPA bear a high degree of similarity in the rationale, core, scope, and the application of the provision considered.

Fairly consistent: The GDPR and the PDPA bear a high degree of similarity in the rationale, core, and the scope of the provision considered; however, the details governing its application differ.

Fairly inconsistent: The GDPR and the PDPA bear several differences with regard to scope and application of the provision considered, however its rationale and core presents some similarities.

Inconsistent: The GDPR and the PDPA bear a high degree of difference with regard to the rationale, core, scope and application of the provision considered.



Usage of the Guide

This Guide is general and educational in nature and is not intended to provide, and should not be relied on, as a source of legal advice. The information and materials provided in the Guide may not be applicable in all (or any) situations and should not be acted upon without specific legal advice based on particular circumstances.

1. Scope

1.1. Personal scope

Both the GDPR and the PDPA protect living persons with regard to the use of their personal data, and apply to data controllers, as well as data processors. Furthermore, while the GDPR applies to public bodies, the PDPA excludes public authorities that maintain state security from its scope, including financial security, security of the state or public safety, including the duties with respect to the prevention and suppression of money laundering, forensic science or cybersecurity.

GDPR	PDPA
Articles 3, 4(1) Recitals 2, 14, 22-25	Sections 4-6, 37(2)

Similarities

GDPR	PDPA
The GDPR **only** protects **living individuals**. The GDPR does not protect the personal data of deceased individuals, this being left to Member States to regulate.	The PDPA **only** protects **living individuals** and expressly excludes information relating to deceased individuals in the definition of personal data.
The GDPR defines a **data controller** as 'a natural and 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.'	The PDPA defines a **data controller** as a natural or juristic person 'who operates in relation to the collection, use, or disclosure of personal data.'
The GDPR defines a **data processor** as a 'natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.'	The PDPA defines a **data processor** as a natural or juristic person 'who operates in relation to the collection, use or disclosure of personal data pursuant to the orders given by or on behalf of a data controller, whereby such a person is not the data controller.'
Article 4(1) of the GDPR clarifies that a **data subject** is 'an identified or identifiable natural person.'	The PDPA refers to **data subjects** throughout, however, does not provide a definition of a data subject.

Differences

GDPR	PDPA
The GDPR **applies** to data controllers and data processors who may be **public bodies**.	The PDPA **does not** apply to public authorities that maintain state security, including financial security of the state or public safety, including the duties with respect to the prevention and suppression of money laundering, forensic science or cybersecurity.

GDPR	PDPA

Differences (cont'd)

The GDPR provides that it 'should apply to natural persons, **whatever their nationality or place of residence**, in relation to the processing of their personal data.'	The PDPA applies to data subjects within Thailand and makes **no explicit reference** to their nationality or place of residence in relation to the processing of personal data.

1.2. Territorial scope

Consistent

With regard to extraterritorial scope, the GDPR applies to data controllers and data processors that do not have a presence in the EU where processing activities take place in the EU. Similarly, the PDPA applies to data controllers and data processors who are outside of Thailand, if their activities consist of offering goods or services to, or monitoring the behaviour of, data subjects in Thailand.

GDPR	PDPA
Articles 3, 4, 11 Recitals 2, 14, 22-25	Section 5

Similarities

The GDPR applies to organisations that have a presence in the EU, notably entities that have an '**establishment**' in the EU. Therefore, the GDPR applies to the processing of personal data by organisations **established** in the EU, regardless of **whether the processing takes place in the EU or not**.

PDPA applies to the collection, use, or disclosure of personal data by organisations that are in Thailand regardless of **whether the collection, use or disclosure of personal data takes place in Thailand or not**.

In relation to **extraterritorial scope**, the GDPR applies to the processing activities of data controllers and data processors that **do not have any presence in the EU**, where processing activities are related to the **offering of goods, or services to individuals in the EU, or to the monitoring of the behaviour of individuals in the EU**.

In relation to **extraterritorial scope**, the PDPA applies to data controllers and data processors that are outside of Thailand where the collection, use or disclosure of personal data of data subjects who are in Thailand, where their activities relate to the **offering of goods or services to data subjects in Thailand**, regardless of whether payment is required or where **the data subject's behaviour is being monitored in Thailand**.

Differences

Not applicable.

Not applicable.

1.3. Material scope

Both the GDPR and the PDPA define personal data as information that directly or indirectly relates to an individual, stipulate specific requirements relating to certain types of data, and apply to the collection, use, and disclosure of personal data. Similarly, both laws provide exceptions for personal data processing that is for legal purposes, for personal use, and for certain artistic and media related purposes.

However, the GDPR and the PDPA do vary regarding other aspects of material scope. The PDPA provides exceptions for legislative bodies and credit bureau companies. Comparatively, the GDPR explicitly excludes anonymous data, and specifies that it applies to the processing of personal data, by automated or non-automated means, if the data are part of a filing system.

GDPR	PDPA
Articles 2, 3, 4, 9, 26 Recitals 15-21, 26	Sections 4, 5, 26

Similarities

The GDPR applies to the '**processing**' of personal data. The definition of 'processing' covers 'any operation' performed on personal data 'such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.'

The PDPA applies to 'the **collection, use or disclosure** of personal data' by a data controller or data processor.

The GDPR defines '**personal data**' as 'any information' that directly or indirectly relates to an identified or identifiable individual. The GDPR does not apply to the personal data of deceased persons.

The PDPA defines '**personal data**' as 'any information relating to a person, which enables the identification of such person, whether directly or indirectly, but not including the information of deceased persons.'

The GDPR defines **special categories of personal data** as personal data revealing **racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation**. The GDPR also provides specific requirements for its processing.

Whilst the PDPA does not define special categories of data, Section 26 requires that explicit consent be obtained for the collection of 'personal data pertaining to **racial, ethnic origin, political opinions, cult, religious or philosophical beliefs, sexual behaviour, criminal records, health data, disability, trade union information, genetic data, biometric data, or of any data which may affect the data subject in the same manner**, as prescribed by the PDPC.'

The GDPR **excludes** from its application the processing of personal data by individuals for **purely personal or**

The PDPA **excludes** from its application 'the collection, use, or disclosure of personal data by a person who

GDPR	PDPA
Similarities (cont'd)	
household purposes. This is data processing that has 'no connection to a professional or commercial activity.'	collects such personal data for **personal benefit or household activity** of such person only.'
The GDPR **excludes** from its application data processing in the context of **law enforcement or national security**.	The PDPA **excludes** from its application '**operations of public authorities having the duties to maintain state security**, including financial security of the state or public safety, including the duties with respect to the prevention and suppression of money laundering, forensic science or cybersecurity [...] **trial and adjudication of courts and work operations of officers in legal proceedings**, legal execution, and deposit of property, including work operations in accordance with the criminal justice procedure.'
The GDPR provides requirements for specific processing situations including processing for **journalistic purposes and academic, artistic or literary expression**.	The PDPA provides for certain processing circumstances including for 'a person or a juristic person who uses or discloses personal data that is collected only for the **activities of mass media, fine arts, or literature**, which are only in accordance with professional ethics or for public interest.
Differences	
The GDPR applies to the processing of personal data **by automated means or non-automated means if the data is part of a filing system**.	The PDPA **does not** differentiate or refer to automated and non-automated means of processing.
The GDPR excludes **anonymous data** from its application, which is defined as information that does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable.	Although the PDPA provides for the right to request that personal data be anonymised, it **does not** explicitly exclude anonymised data from its application.
The GDPR **does not** specifically exclude legislative bodies.	The PDPA excludes from its application '**the House of Representatives, the Senate, and the Parliament**, including

GDPR	PDPA
Differences (cont'd)	
	the committee appointed by the House of Representatives, the Senate, or the Parliament, which collect, use or disclose personal data in their consideration under the duties.'
The GDPR **does not** refer to credit bureau companies and their operations.	The PDPA further excludes 'operations of data undertaken by a **credit bureau company** and its members, according to the law governing the operations of a credit bureau business.'

2. Key definitions

2.1. Personal data

The PDPA and the GDPR both provide the definition of 'personal data,' although the GDPR gives a more detailed definition on the same. In particular, the GDPR provides that IP addresses, cookie identifiers, and radio frequency identification tags may be considered personal data.

In addition, the GDPR provides the definition for sensitive data while the PDPA provides that the collection of certain data requires the consent of the data subject.

GDPR	PDPA
Articles 4(1), 9 Recitals 26-30	Sections 6, 22, 23, 26, 33

Similarities

The GDPR defines '**personal data**' as '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.'

The PDPA defines '**personal data**' as any information relating to a person, which enables the identification of such person, whether directly or indirectly, but not including information of the deceased persons. The PDPA also specifies that a 'person' means a 'natural person.'

The GDPR defines **special categories of personal data** as data revealing a data subject's 'racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.'

The PDPA **does not** define special categories of personal data. However Section 26 requires that explicit consent be obtained for the collection of 'personal data pertaining to **racial, ethnic origin, political opinions, cult, religious or philosophical beliefs, sexual behaviour, criminal records, health data, disability, trade union information, genetic data, biometric data, or of any data which may affect the data subject in the same manner**, as prescribed by the PDPC.'

GDPR	PDPA
Differences	
The GDPR specifies that **online identifiers** may be considered as personal data, such as **IP addresses, cookie identifiers, and radio frequency identification tags**.	The PDPA **does not** specifically address IP addresses, cookie identifiers, and radio frequency identification tags.
The GDPR **does not** apply to 'anonymised' data, where the data can no longer be used to identify the data subject.	Although the PDPA provides for the right to request that personal data be anonymised it **does not explicitly exclude anonymised** data from its application.

2.2. Pseudonymisation

Inconsistent

The GDPR provides a definition for pseudonymised data and it clarifies that such data are subject to the obligations of the GDPR, unlike the PDPA which does not provide a definition of pseudonymised data.

GDPR	PDPA
Articles 4(5), 11 Recitals 26, 28	Section 33

Similarities

GDPR	PDPA
Not applicable.	Not applicable.

Differences

GDPR	PDPA
The GDPR defines **pseudonymised data** as 'the processing of personal data in such a manner that the personal data that can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.'	The PDPA **does not** define pseudonymised data.

2.3. Controllers and processors

Consistent

The GDPR and the PDPA are similar with regard to the scope and responsibilities of data controllers and data processors, and include corresponding definitions and obligations regarding compliance with data subject rights, data breach notifications, record keeping, security measures, and appointing a data protection officer ('DPO').

Both the GDPR and the PDPA require data controllers to implement appropriate security measures and notify supervisory authorities of data breaches.

While the GDPR specifically provides for Data Protection Impact Assessments ('DPIAs') in certain circumstances, the PDPA outlines that data controllers have a duty to provide appropriate security measures and review them when it is necessary, or when the technology has changed in order to effectively maintain the appropriate security and safety standards.

GDPR	PDPA
Articles 4, 17, 28, 30, 32, 33, 35, 37, 38 Recitals 64, 90, 93	Sections 5, 6, 30-41

Similarities

A **data controller** is a natural or legal person, public authority agency or other body that determines the **purposes** and **means** of the processing of personal data, alone or jointly with others.	A **data controller** is a person or a juristic person who has the power and duties to make decisions regarding the collection, use, or disclosure of personal data.
A **data processor** is a natural or legal person, public authority, agency or other body which processes personal data on **behalf** of the controller.	A **data processor** is 'a person or a juristic person who operates in relation to the collection, use or disclosure of the personal data pursuant to the orders given by or on **behalf** of a data controller.'
Data controllers must comply with the **purpose limitation and accuracy principles**, and **rectify** a data subject's personal data if it is **inaccurate** or **incomplete**.	Data controllers should ensure that personal data 'remains **accurate, up-to-date, complete, and not misleading**.' The PDPA also provides that 'the collection of personal data shall be **limited to the extent necessary** in relation to the lawful purpose of the data controller.'
Data controllers must implement **technical and organisational security measures**, and notify supervisory authorities of **data breaches**.	Data controllers or data processors must provide **appropriate security measures** that meet a minimum standard prescribed by the PDPC, and review these measures as necessary. The PDPA also provides that data controllers notify the PDPC of **data breaches**.
Data controllers based outside the EU and involved in certain forms of processing, with exceptions based on the scale of processing and type of data, are obliged to **designate a representative based within the EU** in writing.	Data controllers based outside Thailand and involved in certain forms of data processing, are obliged to **designate a representative based within Thailand** in writing.

GDPR	PDPA
Similarities (cont'd)	
The GDPR stipulates that data controllers and data processors keep **records of processing activities** and provides an exception from this obligation for small organisations. It also provides for the designation of a **DPO** by data controllers or data processors.	The PDPA stipulates that data controllers and data processors **keep records of processing activities** and provides an exception from this obligation for small organisations. It also provides for the designation of **DPOs** by data controllers or data processors.
The GDPR provides that where processing it to be carried out on behalf of a controller, the **controller shall use only data processors providing sufficient guarantees to implement appropriate technical and organisational measures** in such a manner that processing will meet the requirements of the GDPR and ensure the protection of the rights of the data subject. In addition, the data processor shall not engage another data processor without prior specific or general written **authorisation** of the controller.	The PDPA provides that in circumstances where 'personal data is to be provided to other persons or legal persons, apart from the data controller, **the data controller shall take action to prevent such person from using or disclosing such personal data** unlawfully or without **authorisation**.'
The GDPR **does not** specifically refer to an examination system. However, it stipulates that 'time limits should be established by the data controller for **erasure** or for a periodic review' and provides that data controllers should use all reasonable measures to verify the identity of a data subject who requests and should not **retain** personal data for the sole purpose of being able to react to potential requests.	Data controllers are obliged to 'put in place the examination system for **erasure** or destruction' of personal data as necessary to comply with **retention** periods, when data subject withdraws consent, etc.
The GDPR provides that a data controller or data processor conduct **DPIAs** in certain circumstances.	The PDPA **does not** expressly provide for DPIAs. However, Section 37(1) outlines that data controllers have a duty to provide appropriate security measures and review them when it is necessary, or when the technology has changed in order to effectively maintain the appropriate security and safety standards.
Differences	
Not applicable.	Not applicable.

2.4. Children

Fairly Inconsistent

Both the GDPR and the PDPA provide special provisions for protecting children's data, particularly with regard to obtaining consent. Whilst the GDPR provides protections in relation to the provision of information services, the PDPA appears to be wider in scope. Under the GDPR, children under the age of 16 must have their parents' or guardians' consent, with Member States being allowed to lower the age threshold to 13. The PDPA provides that minors who are not *sui juris* by marriage or have no capacity as a *sui juris* person under the Civil and Commercial Code ('the Code'), or are under the age of ten, cannot provide consent. In such case, consent must be granted by the holder of parental responsibility over the child.

Unlike the PDPA, however, the GDPR provides specific requirements when providing information addressed specifically to a child, and states that specific protection should be given when children's personal data is used for marketing or collected for information society services offered directly to a child.

GDPR	PDPA
Articles 6, 8, 12, 40, 57 Recitals 38, 58, 75	Sections 19, 20(1), 20(2)

Similarities

GDPR	PDPA
The GDPR **does not** define 'child' nor 'children.'	The PDPA **does not** define 'child' nor 'children.'
Where the processing is based on consent, the consent of a parent or guardian is required for providing information society services to a child below the **age of 16**. EU Member States can **lower this age limit to 13**.	Where the minor's consent is not any act which the minor may be entitled to provide, as prescribed under the Code, or where the minor is under the **age of 10 years**, consent must be obtained from the holder of the parental responsibility over the child.

Differences

GDPR	PDPA
The GDPR considers children as '**vulnerable natural persons**' that merit specific protection with regard to their personal data. In particular, specific protection should be given when children's personal data is used for marketing or collected for information society services offered directly to a child.	The PDPA **does not** specify whether specific protection should be given when children's personal data is used for marketing or collected for information society services offered directly to a child.
When any information is addressed specifically to a child, controllers must take **appropriate measures** to provide **information** relating to processing in a concise, transparent, intelligible and easily accessible form, using clear and plain language, that the child can easily understand.	The PDPA **does not** outline specific requirements for controllers to take when addressing a child or when providing information to a child.
The GPDR provides that data controllers are required to make reasonable efforts to **verify** that **consent** is given or authorised by a parent or guardian.	The PDPA **does not** specify whether data controllers are required to make reasonable efforts to verify that consent is given or authorised by a parent or guardian.
The GDPR applies to **information services**.	The PDPA appears to be **wider** in its scope.

2.5. Research

Fairly Inconsistent

Under the GDPR, the processing of sensitive data is not prohibited when necessary for research purposes when specific measures have been taken to safeguard the fundamental rights and interests of the data subjects. Similarly, the PDPA outlines that any collection of certain types of data is prohibited without explicit consent except where it is for scientific, historical, or statistical purposes and that suitable measures have been taken to protect the fundamental rights of the data subjects.

Both the GDPR and the PDPA provide data subjects with the right to object to processing unless it is in the public interest.

The GDPR provides specific rules for the processing of personal data for research purposes, including data minimisation and anonymisation. The PDPA does not include specific rules for the collection, use, and disclosure of personal data for such purposes, but requires that 'suitable measures are put in place. In addition, the GDPR provides a definition of scientific research, whereas the PDPA does not.

GDPR	PDPA
Articles 5(1)(b), 9(2)(j), 14(5), 17(3), 21(6), 89 Recitals 33, 159-61	Sections 24, 26, 32

Similarities

According to the GDPR, **the processing of sensitive data is not prohibited when 'necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes**, which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.'

The PDPA states that any collection, use or disclosure of personal data relating to racial, ethnic origin, political opinions, cult, religious or philosophical beliefs, sexual behaviour, criminal records, health data, disability, trade union information, genetic information, biometric data, or any data which may affect the data subject in the same manner is prohibited without explicit consent, **except** where it is for **scientific, historical or statistical purposes** and suitable measure have been taken to **protect the fundamental rights** of the data subjects as prescribed by the PDPC.

The data subject has **the right to object** to the processing of personal data for research purposes **unless such research purposes are for reasons of public interest**.

The data subject has the **right to object** to the collection, use, and disclosure of personal data concerning them if such collection, use, or disclosure is necessary for the purpose of scientific, historical or statistical research **unless carried out for reasons of public interest**.

Differences

Under the GDPR, the processing of personal data for research purposes is subject to **specific rules** (e.g. with regard to the purpose limitation principle, right to erasure, data minimisation and anonymisation etc.).

The PDPA **does not** contain specific rules for the collection, use, or disclosure of personal data for research purposes but data controllers must take suitable measures to protect the data subject's rights, freedoms and interests.

GDPR	PDPA

Differences (cont'd)

The GDPR clarifies that the processing of personal data for **scientific research** purposes should be interpreted 'in a broad manner including for example technological development and demonstration, fundamental research, applied research and privately funded research.'	The PDPA **does not** include a definition for scientific research.
Under the GDPR, where personal data are processed for research purposes, it is possible for Member States to derogate from some data subjects' rights, including the right to access, the right to rectification, the right to object and the right to restrict processing, insofar as such rights are likely to render impossible or seriously impair the achievement of the specific purposes, and such **derogations** are necessary for the fulfilment of those purposes.	The PDPA **does not** include information on the derogation of data subject rights for research purposes.

3. Legal basis

Both the GDPR and the PDPA require a legal basis for processing personal data which include consent, the performance of a contract, legal obligations, public interest, legitimate interest and vital interests or supressing danger to the data subject's life.

The GDPR prohibits the processing of special categories of data unless one of the exceptions applies, including, the data subject's explicit consent. Similarly, the PDPA states that any collection of certain types of data is prohibited except where an exemption applies, such as the data subject's explicit consent.

GDPR	PDPA
Articles 5-10 Recitals 39-48	Sections 19, 24, 26

Similarities

The GDPR states that data controllers can only process personal data when there is a legal ground for it. The legal grounds are:

- **consent**;
- when processing is necessary for the **performance of a contract** which the data subject is part of in order to take steps at the request of the data subject prior to the entering into a contract;
- compliance with **legal obligations** to which the data controller is subject;
- to protect the **vital interest** of the data subject or of another natural person;
- performance carried out in the **public interest** or in the official authority vested in the data controller; or
- for the **legitimate interest** of the data controller when this does not override the fundamental rights of the data subject. Further permissible uses are provided for the processing of special categories of personal data under Article 9(2).

The GDPR recognises **consent** as a legal basis to process personal data and includes **specific information** on how consent must be obtained and can be withdrawn.

Under the GDPR, as a general rule, the processing of **special categories of personal data is restricted unless** an exemption applies, which include the data subject's **explicit consent.**

The PDPA states that data controllers shall not collect, use, or disclose personal data unless the data subject has provided:

- prior **consent**;
- when processing is necessary for the **performance of a contract**;
- is necessary for **compliance with a law** to which the data controller is subjected;
- for **supressing danger to a data subject's life**;
- for the performance of a task carried out in the **public interest** by the data controller the achievement of the purpose relating to public interest research and statistics; or
- for the **legitimate interest** of the data controller where such interest does not override those of the data subject.

The PDPA recognises **consent** as a legal basis to collect, use, or disclose personal data, and includes **specific information** on how consent can be obtained and withdrawn.

The PDPA states that any collection of **personal data** relating to racial, ethnic origin, political opinions, cult, religious or philosophical beliefs, sexual behaviour, criminal records, health data, disability, trade union information, genetic information, biometric data, or any data which may affect

GDPR	PDPA
Similarities (cont'd)	
	the data subject in the same manner **is prohibited except** where an exemption applies, such as the data subject's **explicit consent**.
Differences	
Not applicable.	Not applicable.

4. Controller and processor obligations

4.1. Data transfers

Fairly Consistent

Both the GDPR and the PDPA provides for restrictions and exceptions to the cross-border transfer of personal data to a third country or international organisation. Such a transfer must be made based on legitimate grounds or in accordance with an adequate level of data protection as prescribed by the relevant authority.

In addition, Thailand is in the process of establishing sub-regulations relating to the PDPA for the effective and clear implementation of rights and obligations under the same.

GDPR	PDPA
Articles 44-50 Recitals 101, 112	Sections 28, 29

Similarities

The GDPR allows personal data to be transferred to a third country or international organisation that has an **adequate level of protection** as determined by the EU Commission.

Under the PDPA, the transfer of personal data is only permitted to destination countries or international organisations that have an **adequate level of protection** as prescribed by the PDPC.

Further guidance on what constitutes an adequate level of protection will be published by the PDPC.

One of the following **legal grounds** can be applied to the transfer of personal data abroad:

- when a data subject has explicitly **consented** to the proposed transfer and acknowledged the possible risks of such transfer due to inadequate safeguards;
- when the transfer is necessary for the performance or conclusion of a **contract**;
- when the transfer is necessary for important **public interest** reasons;
- when the transfer is necessary for the establishment, exercise, or defence of a **legal** claim; and
- when the transfer is necessary to protect the **vital interests** of a data subject or other persons.

A cross-border transfer is permitted under the following **legal grounds**:

- where the **consent** of the data subject has been obtained;
- it is necessary to perform an obligation under a **contract** or the transfer is at the request of a data subject;
- it is performed for significant **public interest**;
- the transfer is pursuant to the **law**; and
- where it is to prevent or suppress a **danger to the life**, body, or health of the data subject or other persons, when the data subject is incapable of giving their consent.

GDPR	PDPA

Similarities (cont'd)

In the absence of a decision on adequate level of protection, a transfer is permitted when **the data controller or data processor provides appropriate safeguards** with effective legal remedies that ensure the data subjects' rights as prescribed under the GDPR. **Appropriate safeguards include**:

- binding corporate rules with specific requirements (e.g. a legal basis for processing, a retention period, complaint procedures, etc.);
- standard data protection clauses adopted by the EU Commission or by a supervisory authority;
- an approved code of conduct; or
- an approved certification mechanism.

In addition, during the establishment of an adequate level of protection, as well as personal data protection policy, the data controller or data processor is permitted to transfer personal data abroad only in case where there are **appropriate safeguards** in place with effective legal remedies that ensure the data subjects' rights as prescribed by the PDPC.

In the absence of an adequate level of protection, a transfer is permitted when the personal data **is transferred to affiliates of a national data controller or data processor that apply a personal data protection policy** approved by the PDPC.

The PDPA **has not yet established the criteria of personal data protection policy** nor has it established the scope of 'affiliates' for the implementation of the above requirement.

Differences

The GDPR specifies that a cross-border transfer is allowed based on **international agreements** for judicial cooperation.

The grounds for a cross-border transfer includes the **transfer being made from a register** which, according to the Union or a Member States' law, is intended to provide information to the public, and which is open to consultation either by the public in general or by any person who can demonstrate a **legitimate interest**, but only to the extent that the conditions laid down by Union or Member State law for consultation are fulfilled in the particular case.

The PDPA **does not** specifically address the transfer of personal data for the purpose of complying with a court judgment or any decision of a third country's authority.

The PDPA **does not** recognise a cross-border transfer that is made from a register that is intended to provide information to the public, or by any person who can demonstrate a **legitimate interest**.

4.2. Data processing records

Fairly Consistent

Both the GDPR and the PDPA have imposed an obligation on data controllers and data processors to record their processing activities. In both laws, this obligation also applies to the representative of a data controller and the lists of information that must be retained bear many similarities.

The GDPR describes a list of information that a data processor must record while the PDPA does not.

GDPR Article 30 Recital 82	PDPA Sections 39, 40

Similarities

Data controllers and data processors have an obligation to **maintain a record** of processing activities under their responsibility.

Data controllers and data processors are required to **maintain a record** of their personal data processing activities.

The GDPR **prescribes a list of information that a data controller** must record:

- the name and contact details of the **data controller**;
- the **purposes of the processing**;
- a description of the categories of **personal data**;
- the categories of recipients to whom the personal data will be **disclosed**;
- the **estimated period for erasure** of the categories of data; and
- a general description of the technical and organisational **security measures** that have been adopted.

The PDPA **prescribes the specific information that a data controller** must record for the verification of data subjects and the competent authority, which includes:

- the information of the **data controller**;
- the **purposes of the processing**;
- the details of collected **personal data**;
- the rights and means to **access** the data subjects' personal data, including conditions of access and person(s) authorised to access such data;
- the **retention** period of the personal data; and
- a general description of **security measures**.

The obligations in relation to data processing records are also imposed on the **representatives of data controllers**.

In the case that a data controller is a foreign entity, such entity is required to designate a local representative in Thailand. The local **representative of the data controller** is obligated to perform activities on behalf of the data controller, including recording their processing activities in the same manner as the data controller.

The processing on information recorded by a data controller shall be **in writing or electronic form**.

The processing of information of a data controller can be recorded in **writing or electronic form**.

GDPR	PDPA

Similarities (cont'd)

The requirements around data processing records shall not apply to **an organisation with less than 250 employees**, unless the processing:

- is likely to result in a risk to the rights and freedoms of data subjects;
- is not occasional; or
- includes special categories of data in Article 9(1) (e.g. religious beliefs, ethnic origin, etc.) or is personal data relating to criminal convictions and offences in Article 10.

The requirements around data processing records shall not apply to a **small organisation**, unless the processing:

- is likely to result in a risk to the rights and freedoms of data subjects;
- is not occasional; or
- includes special categories of data in Section 26 (e.g., religious beliefs, ethnic origin, data required for the establishment, exercise, or defence of legal claims, etc.).

Differences

The GDPR **prescribes a list of information that a data processor** must record:

- the name and contact details of the data processor;
- the categories of processing carried out on behalf of each controller;
- international transfers of personal data, with the identification of third countries or international organisations, and the documentation of adopted suitable safeguards; and
- a general description of the technical and organisational security measures that have been adopted.

The PDPA **does not** specify a list of processing information that a data processor must record.

However, as mentioned in Section 40, notification(s) from the relevant authority relating to data processing records will be published in the future.

The GDPR **prescribes a list of information that a data controller** must record **international transfers** of personal data, with the identification of third countries or international organisations, and the documentation of adopted suitable safeguards.

The PDPA **does not** explicitly prescribe that a data controller must record international transfers of personal data.

4.3. Data protection impact assessment

The GDPR specifically provides for DPIAs in certain circumstances. Although the PDPA does not specifically refer to DPIAs, it does provide that data controllers have a duty to provide appropriate security measures and review them when it is necessary, or when the technology has changed in order to effectively maintain the appropriate security and safety standards.

GDPR	PDPA
Articles 35-36 Recitals 75, 84, 89-93	Sections 37, 40

Similarities

Under the GDPR, a **DPIA must be conducted** under specific circumstances.

Under the PDPA, appropriate **security measures should be adopted and reviewed** when it is necessary, or when the technology has changed in order to effectively maintain the appropriate security and safety standards.

A data controller is required to, **where necessary**, carry out a review to assess whether the processing of personal data is in accordance with the DPIA, **particularly when there is a change** in risks to processing operations.

Under the PDPA, a data controller must establish security measures (with minimum standards as prescribed by the PDPC) to prevent the loss, access, use, change, revision or disclosure of personal data without authorisation. The assessment of such security measures for processing operations shall be performed **when deemed necessary or there is a change** in the technology of security measures.

The GDPR provides that a DPIA must be conducted if a data controller utilises **new technologies** to process personal data.

The PDPA provides that a security assessment shall be conducted where there is a **change in technology** related to security measures.

Differences

The GDPR provides that a DPIA must be conducted **under the following circumstances**:

- the processing may result in a high risk to the rights and freedoms of an individual;
- when a systematic and extensive evaluation of personal aspects relating to natural persons is involved, which is based on automated processing or profiling;
- there is processing on a large scale of special categories of data; and

In order to comply with minimum standards as prescribed by the PDPC, an assessment of security measures for processing operations shall be conducted **only when it is deemed necessary, or there is a change in technology**. The PDPA provides that a minimum standard will be specified by the PDPC.

GDPR Portal

The most comprehensive resource for the development and maintenance of your GDPR programme.

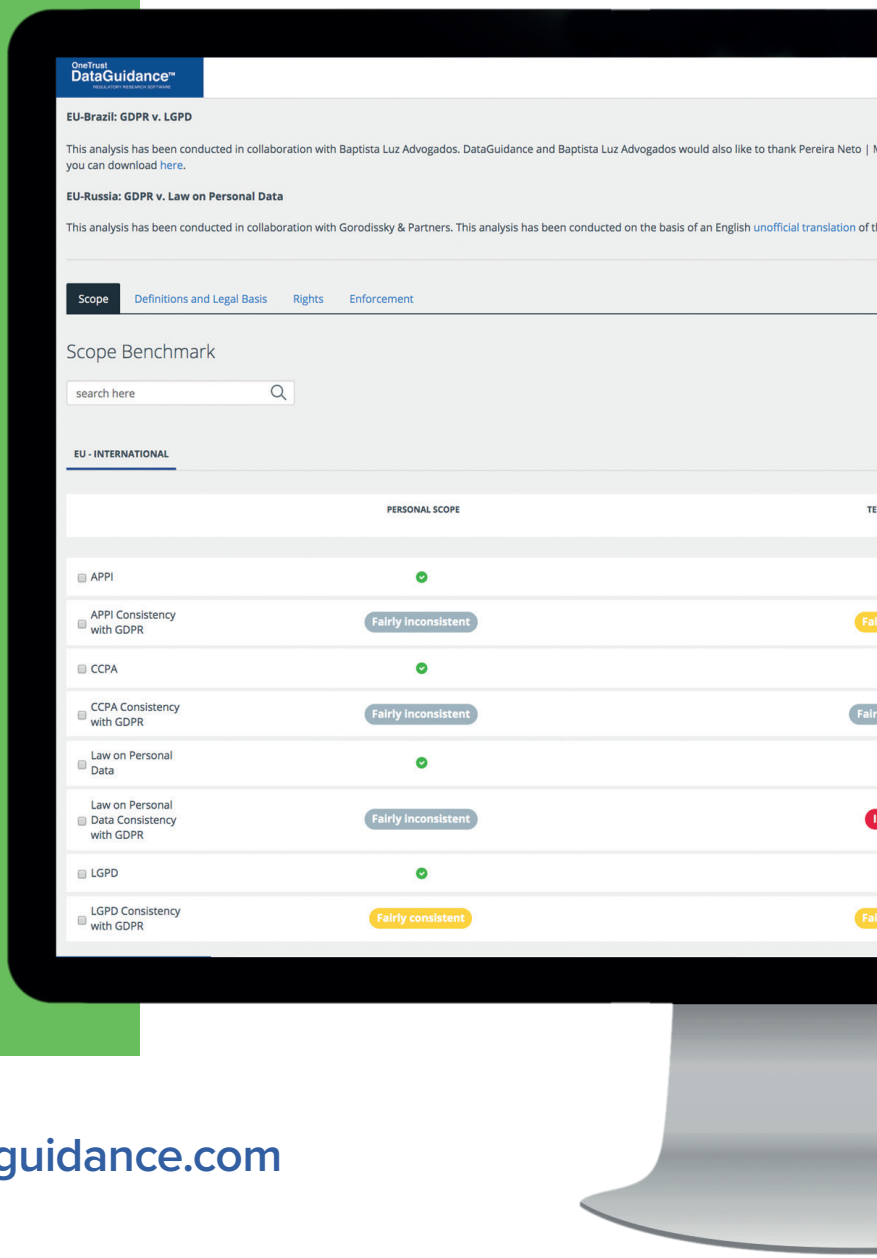
- Understand obligations and requirements across key topics and sectors
- Track developments regarding Member State implementation and regulatory guidance
- Apply expert intelligence to make business decisions
- Utilise GDPR specific checklists and templates

OneTrust
DataGu
REGULATORY

Global Regulatory

40 In-House Legal Researchers, 50

Monitor regulatory dev
and achieve glo



Sign up for a free trial at **dataguidance.com**

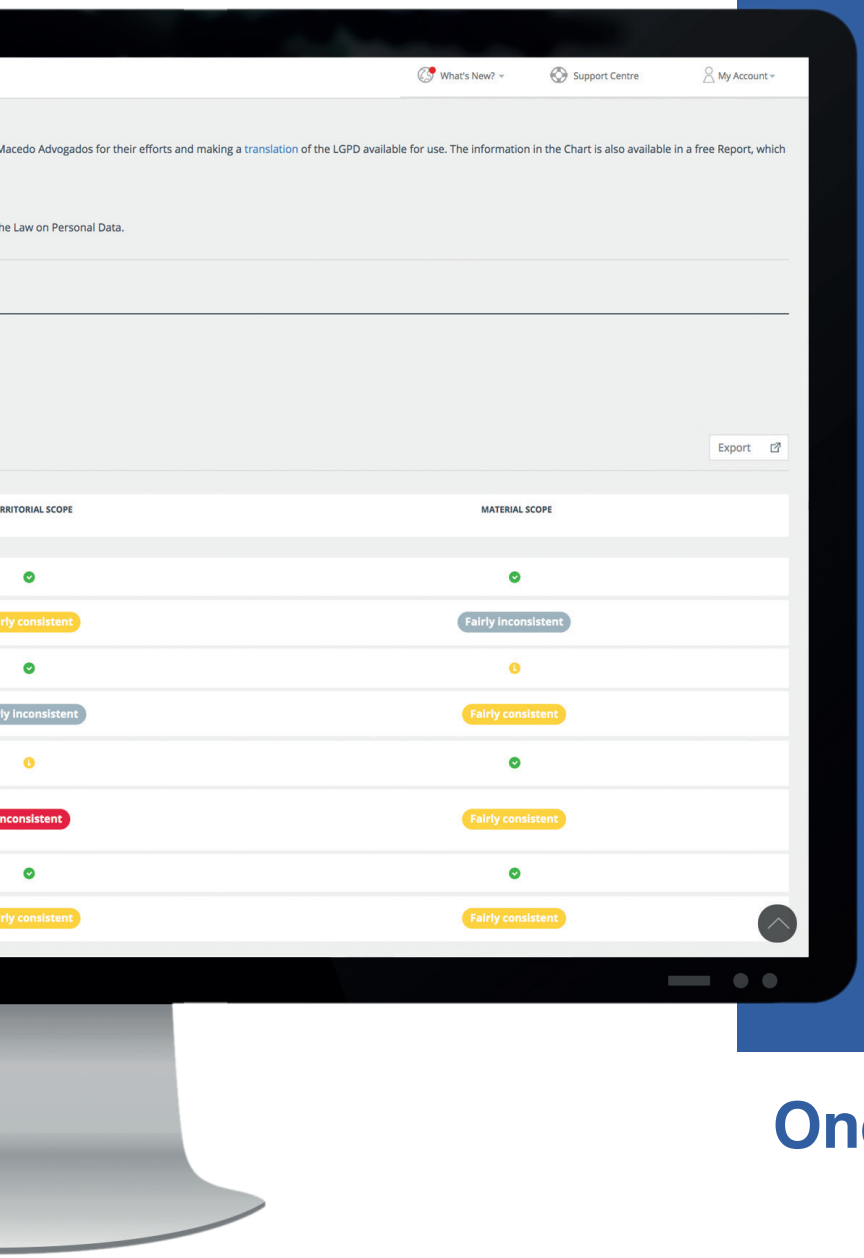
idance™

RESEARCH SOFTWARE

Research Software

00 Lawyers Across 300 Jurisdictions

elopments, mitigate risk
bal compliance.



GDPR Benchmarking

Understand and compare key provisions of the GDPR with relevant data protection law from around the globe.

- Compare requirements under the GDPR to California, Japan, Brazil, Russia and Thailand with a dedicated comparative tool
- Employ topic specific guidance to develop your compliance activities
- Monitor news and access written opinion pieces on the most recent developments

OneTrust DataGuidance™
REGULATORY RESEARCH SOFTWARE

GDPR	PDPA
Differences (cont'd)	
• there is systematic monitoring of a publicly accessible area on a large scale.	
The assessment **must contain at least** the following: • a systematic description of the envisaged processing operations and legitimate purposes of the processing; • the necessity and proportionality of the operations in relation to the purposes; and • the risks to the rights and freedoms of data subjects.	The scope of assessment **is not provided for** in the PDPA.
A data controller **must consult** the supervisory authority prior to any processing that would result in a high risk in the absence of risk mitigation measures as indicated by the DPIA.	The PDPA **does not** require the data controller to consult the authority with regard to any processing of personal data.

4.4. Data protection officer appointment

Consistent

Both the GDPR and the PDPA require data controllers and data processors, including their representatives, to designate a DPO. The nature and scope of the DPO's tasks are included under both the GDPR and the PDPA.

GDPR	PDPA
Articles 13-14, 37-39 Recital 97	Sections 29, 41, 42

Similarities

Under the GDPR, data controllers and data processors, including their representatives, are required to **appoint** a DPO.

The data controller and the data processor shall designate a DPO in any case where:

- the processing is **carried out by a public authority or body**, except for courts acting in their judicial capacity;
- the core activities of a data controller or data processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require **regular and systematic monitoring** of data subjects on a large scale; or
- the core activities of the controller or the processor relate to a large scale of **special categories of personal data** (e.g. religious beliefs, ethnic origin, data required for the establishment, exercise, or defence of legal claims etc.)

A group may appoint a **single DPO** who must be easily contactable by each establishment.

Where the data controller or the data processor is a public authority or body, a single DPO can also be appointed for **several public authorities or bodies**, taking into account their organisational structure and size.

Under the PDPA, data controllers and data processors, including their representatives, are required to **appoint** a DPO.

The DPO must be appointed under either of the following general circumstances:

- the processing is **carried out by a public authority or body**;
- the activities of a data controller or data processor relating to collection, use, or disclosure **require regular monitoring** of the personal data or the system on a large scale; or
- the core activities of a data controller or data processor relate to the collection, use, or disclosure of **certain categories of data** (e.g. racial, ethnic origin, political opinions, cult, religious or philosophical beliefs, sexual behaviour, criminal records, health data, disability, trade union information, genetic data, biometric data, or of any data which may affect the data subject in the same manner, as prescribed by the PDPC).

In the case where a data controller and a data processor are members of the same business, an appointment of a **single DPO** is permitted provided that the data protection office is easily accessible for both the data controller and data processor.

The appointment of a single DPO is also permited for **public authorities or bodies** (which are the data controllers or data processors) that have a large organisational structure or several establishments.

GDPR	PDPA

Similarities (cont'd)

The DPO shall perform a list of tasks including; • **to inform and advise** the controller or the data processor and the employees who carry out processing of their obligations pursuant to the GDPR and to other Union or Member State data protection provisions; • **to monitor** compliance with the GDPR with other Union or Member State data protection provisions and with the policies of the data controller or data processor in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits; and • **to act as a contact point** the supervisory authority on issues relating to processing, including the prior consultation referred to in Article 36, and to consult, where appropriate, with regard to any other matter.	The scope of the DPO's duties are: • **to inform and advise** the data controller, data processors, and their employees on obligations under the PDPA; • **to monitor** the performance of the controller or the data processor including their employees or service providers, with processing operations of the data controller, data processors, and their employees; and • **to act as a contact point** for data controllers and data processors.
The DPO shall be designated on the basis of **professional qualities and expert knowledge** of data protection law and practices.	The appointment of the DPO must be considered based on **expert knowledge and expertise** in personal data protection, which may be further specified by the PDPC.
The DPO can be a **staff member** of the data controller or data processor, or can perform tasks based on a **service contract**.	**A staff member** of a data controller or data processor or a contractor under **a service contract** can be designated as the DPO.
Contact details of the DPO must be included in the privacy notice for data subjects, and they must be communicated to the supervisory authority.	Data subjects and the PDPC must be informed of the **contact details** of the DPO.
Data subjects **may contact** the DPO with regard to the processing of their personal data as well as the exercising of their rights.	Data subjects **may contact** the DPO with regard to the collection, use, and disclosure of personal data, including the exercise of their rights.
The DPO must be **provided with the resources necessary** to carry out his or her obligations under the GDPR.	The data controller and data processor must **provide the necessary resources** as well as aid in the facilitation of the DPO's tasks under the PDPA.

GDPR	PDPA
Differences	
As mentioned above, the DPO must be appointed in a case where the processing is carried out by **any** public authority or body.	A list of public authorities or bodies that require the appointment of a DPO will be **specifically published** in a supplemental notification of the PDPC.
The GDPR recognises the **independence** of DPOs.	The PDPA **does not** explicitly comment on the independence of DPOs.

4.5. Data security and data breaches

Both the GDPR and the PDPA include an obligation for data controllers and data processors to adopt security measures.

In addition, the two pieces of legislation impose an obligation to notify the data protection authority, as well as data subjects of any personal data breaches, within 72 hours. However, the GDPR provides exemptions to this obligation in specific circumstances while no such exemptions are currently provided for in the PDPA.

Additional details for the implementation of data security measures, including data breach notifications under the PDPA, will be further established in the supplemental notification(s) issued by the PDPC.

GDPR	PDPA
Articles 5, 24, 32-34 Recitals 74-77, 83-88	Sections 24-26, 37, 40

Similarities

The GDPR recognises **integrity** and **confidentiality as fundamental principles** of protection by stating that personal data must be processed in a manner that ensures appropriate security of the personal data.

The PDPA recognises **security measures as a fundamental principle** for the protection of data subjects' rights and freedoms.

The GDPR states that **data controllers and data processors are required to implement appropriate technical and organisational security measures** to ensure that the processing of personal data complies with the obligations of the GDPR.

The PDPA states that **data controllers and data processors must provide appropriate security measures** in order to prevent the loss, access, use, change, revision, or disclosure of personal data without authorisation.

In the case of a personal data breach, the **data controller must notify the competent supervisory authority** of the breach, unless the personal data breach is **unlikely to result in a risk** to the individuals' rights and freedoms.

In the case of a personal data breach, the data controller must notify the PDPC of the breach, **except where the personal data breach is unlikely to result in a risk** to individuals' rights and freedoms.

Under the GDPR, a personal data breach must be notified to the supervisory authority **without undue delay** and, where feasible, **no later than 72 hours** after having become aware of the breach.

Under the PDPA, a personal data breach must be notified to the PDPC **without undue delay** and, where feasible, **no later than 72 hours** after having become aware of the breach.

The controller must **notify** the **data subject** of a data breach without undue delay if the data breach is likely to result in a **high risk** to the rights and freedoms of natural persons.

Under the PDPA, if a personal data breach **is likely to result in a high risk** to data subjects' rights and freedoms, the data controller **must notify the breach to data subjects**.

GDPR	PDPA
Differences	
Under the GDPR, the obligation of data controllers to notify data subjects when the data breach is likely to result in a high risk to the rights and freedoms of natural personals, **is exempted in certain circumstances** such as where: • appropriate technical and organisational protective measures have been implemented; • any subsequent measures have been taken in order to ensure that the risks are no longer likely to materialise; or • it would involve disproportionate effort.	Currently, the PDPA **does not** provide any exemptions to the requirement that data controllers notify data subjects of serious personal data breaches. However, a specific exemption(s) will be prescribed in the future in a supplemental regulation(s) of the PDPC.
The GDPR **provides a list of information** that must be, at minimum, **included in the notification** of a personal data breach. For example, a notification must describe the nature of the breach, the approximate number of data subjects concerned, and the consequences of the breach.	Currently, the PDPA **does not** provide requirements for the notification of personal data breaches. However, such a requirement will be prescribed in the future in a supplemental regulation(s) of the PDPC.
The GDPR provides a **list** of **technical and organisational measures**, where appropriate, that data controllers and data processors must implement such as pseudonymisation, encryption and the ability to restore availability and access to personal data in a timely manner in the event of physical or technical incidents, to ensure integrity and confidentiality.	The PDPA **does not** provide a list of technical and organisational measures. However, the PDPA will provide a list of security measures for personal data protection in supplemental regulation(s) of the PDPC.
The GDPR states that **data processors must notify** the data controller without **undue delay** after becoming aware of the personal data breach	The PDPA states that **data processors must notify** data controllers of personal data breaches that have occurred but **does not** specify a timeframe.

4.6. Accountability

Fairly Consistent

While the GDPR recognises accountability as a fundamental privacy principle, the PDPA contains provisions that accountability can be taken to apply to, such as providing an appropriate level of security and appointing DPOs.

GDPR	PDPA
Articles 5, 24-25, 35, 37 Recital 39	Sections 37, 39

Similarities

The GDPR recognises **accountability** as a fundamental principle of data protection. Article 5 states that 'the data controller shall be responsible and able to demonstrate compliance with, paragraph 1 [accountability].'
In addition, the principles can be taken to apply to several other principles as mentioned in other sections of this report, including the appointment of a DPO, and DPIAs.

The PDPC does not expressly address accountability as a fundamental principle. However, it does include **provisions that accountability can be taken to apply to**, such as the adoption of security measures to prevent the loss, access, use, change, revision, or disclosure of personal data without authorisation, the appointment of a DPO, and DPIAs.

Differences

Not applicable.

Not applicable.

5. Individuals' Rights

5.1. Right to erasure

Fairly Consistent

Both the GDPR and the PDPA allow data subjects to request for their personal information to be deleted, unless exceptions apply. The scope of, and exemptions to, the right to erasure are similar between the GDPR and the PDPA. The main difference is in the applicability of the right, for instance, the forms of request and response timelines, which vary between these two pieces of legislation.

GDPR	PDPA
Articles 12, 17 Recitals 59, 65-66	Sections 23(6), 33

Similarities

The right to erasure applies to specific grounds, such as where **consent of the data subject is withdrawn** and there is with **no other legal ground** for processing, or the personal data **is no longer necessary** for the purpose of which it was collected.	The right to erasure under PDPA Section 33 applies where the **consent of a data subject is withdrawn** and the **data controller has no legal ground** to collect, use, or disclose the personal data, or the personal data **is no longer necessary** for the purpose of which it was collected.
The right can be exercised **free of charge**. There may be some instances, however, where a fee may be requested, notably when requests are unfounded, excessive, or have a repetitive character.	The right can be exercised **free of charge**. The data controller must be responsible for all costs.
Data subjects **must be informed** that they have the right to request for their data to be deleted, and are entitled to ask for their data to be erased.	The data controller **must inform** data subjects of the right to request for their personal data to be deleted.
If the data controller has made personal data public and is obliged to erase the personal data, the data controller, taking into account the available technology and the cost of implementation, shall take reasonable steps, including **technical measures**, to **inform controllers** processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data.	Where the data controller has made the personal data public and is requested to erase, destroy, or anonymise such data, the data controller is responsible for applying the necessary **technical measures** and expenses to fulfil the request, as well as **inform others** including any **relevant data controllers** in order to obtain their responses to respond to the request for deletion.

GDPR	PDPA

Similarities (cont'd)

GDPR	PDPA
Exceptions to the right of erasure provided by the GDPR include: • **freedom of expression** and freedom of information; • complying with **public interest purposes in the area of public health**; • establishment, exercise, or defence of **legal claims**; and • **complying with legal obligations** for a public interest purpose.	Similar to those of the GDPR, exceptions to the right of erasure provided by the PDPA include: • **freedom of expression** and freedom of expressing opinion; • complying with **public interest purposes in the areas of public health**, historical archives, or educational research and statistics, subject to sufficient protective measures to protect personal data; • establishment, exercise, compliance with, or defence of, **legal claims**; and • **complying with legal obligations** for a public interest purpose.

Differences

GDPR	PDPA
Data subject requests under this right must be replied to without 'undue delay and in any event within **one month** from the receipt of request.' The deadline can be extended by **two additional months** taking into account the complexity and number of requests. In any case, the data subject must be informed of such extension within one month from the receipt of the request.	**No timeline is specified** for a data controller to respond to a request. However, the PDPA provides data subjects the right to make a complaint to the relevant authority in case the data controller fails to respond to the request for deletion. Notification(s) from the relevant authority relating to conditions on the deletion, which may include a specific timeline, may be published in the future as mentioned in Section 33.
A data controller must have in place **mechanisms** to ensure that the request is made by the data subject whose personal data is to be deleted.	A data controller **is not obligated to put in place mechanisms** to identify a data subject who makes a request for the deletion of his or her personal data.
A request can be made in **writing, orally, and through other means including electronic means** where appropriate.	Specific methods for data subjects to submit a request for the deletion of their personal data are not addressed. Notification(s) from the relevant authority relating to conditions on the deletion, which may include methods to submit a request, may be published in the future as mentioned in Section 33.

5.2. Right to be informed

Both the GDPR and the PDPA recognise the transparency principle. These two laws impose an obligation on a data controller to inform data subjects of specific information relating to the collection and processing of personal data. However, the PDPA does not explicitly specify in what form the right can be exercised.

GDPR	PDPA
Articles 5-13, 14, 47 Recitals 58-63	Sections 19, 21, 23-25, 27, 28, 31, 41, 73

Similarities

Data subjects must be provided with information relating to the processing of personal data in order to validate their consent, including:

- **details of personal data** to be processed;
- **purposes** of processing, including the legal basis for processing;
- **data subjects' rights** (e.g. the right to erasure, right to object, right of withdrawal, right to lodge a complaint to a relevant authority, etc.);
- **data retention period**;
- **recipients or their categories** of personal data; and
- **contact details** of the data controller or its representative and the DPO.

In addition, data subjects must be informed of the **possible consequences** of a failure to provide personal data whether in complying with statutory or contractual requirements, or a requirement necessary to enter into a contract.

Information can be provided to data subjects in an easily accessible form with clear and plain language, which can be in **writing and other means such as electronic format**.

Data subjects must be provided with information relating to the processing of personal data in order to validate their consent.

The PDPA states that information that must be provided to data subjects includes:

- **details of personal data** to be collected, used or disclosed;
- **purposes** of collection for use or disclosure of the personal data, including the legal basis for the collection (no consent required);
- **data subjects' rights** (e.g., the right to erasure, right to object, right of withdrawal, etc.);
- **data retention period**;
- **categories or entities**, either as an individual or organisation, that the personal data will be disclosed to; and
- **contact details** of the data controller or its representative and the DPO.

A data controller is obligated to inform data subjects of the **possible consequences** of not providing their personal data whether such provision is statutory, a contractual requirement, or a requirement necessary to enter into a contract.

Data subjects must be informed of the purpose of processing in an easily accessible form with clear and plain language, which can be in **writing or electronic format**, to obtain the data subjects' consent.

A specific or standard form may be further prescribed by the relevant authority.

GDPR	PDPA

Similarities (cont'd)

A data controller cannot collect and process personal data for purposes other than the ones about which the data subjects were informed, **unless the data controller provides them with further information**.	Data subject(s) **must be informed** of any change to the original processing purpose.
A data controller must **inform** data subjects of the existence or absence of an adequacy decision, or in the case of transfers referred to in Article 46 or 47, or the second subparagraph of Article 49(1), reference the **appropriate or suitable safeguards** and the means by which to obtain a copy of them or where they have been made available.	A data controller must **inform** data subjects of **inadequate privacy safeguards** of a third country or international organisation to which their personal data will be transferred to for their consent to the proposed transfer.
The GDPR provides specific information that must be given to data subjects when their personal data has been **collected from a third party**, which includes the sources from which the data was collected.	The PDPA prescribes that a data controller must provide specific information to data subjects when their personal data is **collected from a third party**, which includes the source from which the data was collected for their consent.
In the case of indirect collection, a data controller must provide information relating to such collection to data subjects within a reasonable period after obtaining the data, but at the latest within one month, or **at the time of the first communication with the data subject, or when personal data is first disclosed to the recipient**.	In the case of indirect collection. The data controller must provide information relating to such collection to data subjects within a reasonable period, but **at the latest within 30 days from the date of collection, or at the time of the first communication with the data subject, or when personal data are is first disclosed to the recipient**.
Information relating to personal data processing (e.g. the purpose of the processing, the rights of data subjects, etc.) must be provided to data subjects by the data controller **at the time when personal data is obtained**.	A data controller is allowed to provide a data subject with information relating to the personal data processing (e.g. the purpose of the processing, the rights of data subjects, etc.) either **before or at the time of personal data collection**.

Differences

Data subjects must be informed of the existence of **automated decision-making, including profiling**, at the time when personal data is obtained.	The PDPA **does not** address the right of data subjects to be informed regarding the existence of automated decision-making and profiling.
Information can be provided to data subjects **orally**, in addition to in writing form or electronic means.	It is **not explicitly specified** whether information can be provided orally.
The GDPR **provides examples** of circumstances, which can be considered as 'legitimate interest.'	The PDPA **does not** provide examples of legitimate interest circumstances.

5.3. Right to object

Fairly Consistent

Both the GDPR and the PDPA guarantee the right for data subjects to object to the processing of their personal data as well as to withdraw their consent to the processing at any time. Both laws clearly specify similar exceptions to the right to object.

Nevertheless, the PDPA provides a more specific scope of application for data subjects.

GDPR Articles 7, 12, 18, 21	PDPA Sections 19, 23, 32

Similarities

Data subjects shall have the right to **withdraw** their consent to the processing of their personal data **at any time**.

The consent of data subjects to the processing of their personal data can be **withdrawn at any time**.

Under the GDPR, data subjects are provided with the right to object to the processing of their personal data in specific circumstances:

- the processing of personal data is due to **tasks carried out in the public interest** or **based on a legitimate interest pursued by the data controller** or **third party**;
- the processing of personal data is for **direct marketing purposes**; and
- the processing of personal data is for **scientific, historical research or statistical purposes**.

Under the PDPA, data subjects shall have the right to object to the processing of their personal data under specific circumstances:

- personal data that is collected without consent due to **tasks carried out in the public interest** or **based on a legitimate interest pursued by the data controller** or **third party**;
- the processing of personal data is for **direct marketing purposes**; and
- the processing of personal data is for **scientific, historical or statistic research purposes**.

The data subject has the right to be **informed** about the right to object.

The data subject has the right to be **informed** about the right to object.

Upon the receipt of an objection request, a data controller shall no longer process the personal data unless:

- **the processing is based on a legitimate ground** that overrides the data subjects' interests; or
- **it is for the establishment, exercise, or defence of a legal claim**.

A data controller can make an objection to the request of data subjects, and continue to collect, use, and disclose their personal data based on two grounds:

- the controller can demonstrate that the collection, use, and disclosure of personal data is **based on a legitimate ground that overrides the data subjects' interests**; or
- the collection, use, and disclosure of personal data has the purpose **of establishing, exercising, or defending against a legal claim**.

Differences

Data subjects must be informed of information about **how to exercise** the right.

The PDPA **does not** explicitly specify whether a data controller has an obligation to provide information to data subjects on how to exercise the right.

GDPR	PDPA

Differences (cont'd)

A request to restrict the processing of personal data must be responded to without undue delay and in any event within **one month** from the receipt of request. The deadline can be extended by **two additional months** taking into account the complexity and number of requests.

The PDPA **does not** specify a timeline for a data controller to respond to a request to restrict the processing of personal data. However, the PDPA provides a right to data subjects to make a complaint to a relevant authority in case the data controller fails to respond to the request of objection.

5.4. Right to access

Fairly Inconsistent

Both the GDPR and the PDPA provide data subjects with the right to access their personal data when it has been collected and processed by a data controller.

However, the laws have several differences with regard to the implementation of the right to access. For example, even though the right to access, recognised under both pieces of legislation, must be notified to data subjects by the data controller, the time period for such notification is different. More differences can be found in the timelines for responses to, as well as the grounds for, refusing requests for access.

GDPR	PDPA
Article 15 Recitals 59-64	Section 30

Similarities

The GDPR recognises that data subjects have the **right to access** their personal data that is processed by a data controller.

Under the PDPA, data subjects have the right to **request access** to their personal data that is processed by a data controller.

The GDPR provides that the right of access must not **adversely affect the rights or freedoms of others**.

Under the PDPA, the right to access personal data and request a copy of such data must not **adversely affect the rights or freedoms of others**.

Differences

The GDPR specifies that, **when responding to an access request**, the data controller must indicate the following information:

- the **purposes** of the processing;
- the **categories** of personal data concerned;
- the recipients or categories of recipients to whom the personal data has been or will be **disclosed**, in particular recipients in third countries or international organisations;
- where possible, the envisaged **period** for which the personal data will be **stored**, or, if not possible, the criteria used to determine that period;
- the existence of the right to request from the controller **rectification or erasure** of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;
- the right to lodge a **complaint** with a supervisory authority;

The PDPA **does not** prescribe what needs to be included in responding to an access request.

GDPR	PDPA

Differences (cont'd)

• where the personal data are not collected from the data subject, any available information as to their **source**; and • the existence of **automated decision-making**, including profiling.	
A data controller can refuse to act on a request when it is **manifestly unfounded, excessive, or has a repetitive character**.	A data controller is allowed to refuse a request to access personal data, including obtaining a copy and/or source of personal data, only in the case where the refusal **complies with law or a court order**.
The GDPR provides that the right of access must not adversely affect the rights or freedoms of others, **including those related to trade secrets**.	Under the PDPA, there is **no exception for those related to trade secrets**.
Data subjects' requests under this right must be replied to without 'undue delay and in any event within one month from the receipt of a request.' The deadline can be extended by **two additional months** taking into account the complexity and number of requests. In any case, the data subject must be informed of such an extension within one month from the receipt of a request.	A data controller must respond to the request without undue delay, and within a maximum of 30 days upon the receipt of the request **with no extension period**. However, as mentioned in Section 30, notification(s) from the relevant authority relating to the exercise of rights as well as an extension period may be published in the future.
The right to access can be exercised **free of charge**. There may be some instances where a fee may be requested, notably when the requests are unfounded, excessive, or have a repetitive character.	The PDPA **does not** specify whether the exercise of this right is free of charge.
Data subjects must have a variety of means through which they can make their request, including **orally and through electronic means**. In addition, when a request is made through electronic means, a data controller should submit a response through the same means.	The PDPA **does not** address the means for data subjects to make a request to access their personal data. However, as mentioned in Section 30, notification(s) from the relevant authority relating to the exercise of rights, which may include the cost of implementation, may be published in the future.
The GDPR specifies that a data controller must **have in place mechanisms** to identify that a request is made by a data subject whose personal data is to be deleted.	The PDPA **does not** impose on a data controller to put in place **mechanisms** to identify a data subject who makes a request to delete his or her personal data.

5.5. Right not to be subject to discrimination in the exercise of rights

The right not to be subject to discrimination in exercising rights is not explicitly mentioned in the GDPR or the PDPA. However, this right can be implied from the fundamental rights of data subjects specified in both legislations.

GDPR	PDPA

Similarities

GDPR	PDPA
The GDPR **does not** explicitly address the right not to be subject to discrimination; therefore, no scope of implementation is defined.	The PDPA **does not** explicitly recognise the right not to be subject to discrimination; therefore, no scope of implementation is defined.

Differences

GDPR	PDPA
Not applicable.	Not applicable.

5.6. Right to data portability

Fairly Consistent

Both the GDPR and the PDPA recognise the right to data portability. Under these two laws, data subjects have the right to receive their personal data in a structured, commonly used, and machine-readable format as well as to transmit such data to other third parties.

GDPR	PDPA
Article 12, 20, 28 Recital 68, 73	Section 24, 31

Similarities

GDPR	PDPA
The GDPR **provides** data subjects with the right to data portability.	The PDPA **provides** data subjects with the right to data portability.
Data subjects have the right to receive their personal data **in a structured, commonly used, and machine-readable format** when the processing is based on consent, contract, or automated means.	Data subjects have right to receive their personal data **in a structured, commonly used, and machine-readable format** when the processing is based on consent, contract, or a legitimate ground.
Data subjects have the right **to transmit** their personal data in the aforementioned form directly to another controller, **where technically feasible**.	Data subjects have the right to request a data controller to, **where technically feasible**: (i) **transmit** their personal data in the aforementioned form directly to another controller; or (ii) provide the transmitted data to (i) above.
The GDPR provides that the right to data portability **must not adversely affect the rights or freedoms of others**.	Under the PDPA, the right to data portability **must not adversely affect the rights or freedoms of others**.

Differences

GDPR	PDPA
The GPDR **does not** explicitly impose an obligation on a data controller to record the ground of objection to a data portability request.	The data controller has an obligation to record **the ground of objection to a data portability request** for the verification of data subjects and the competent authority.

6. Enforcement

6.1. Monetary penalties

Both the GDPR and the PDPA provide for monetary penalties to be issued in cases of non-compliance. However, the amounts differ significantly, and the PDPA outlines both criminal and non-criminal penalties, whereas the GDPR only outlines administrative penalties for non-compliance.

GDPR	PDPA
Articles 83-84 Recitals 148-152	Sections 79-90

Similarities

The GDPR provides for **monetary penalties** in case of non-compliance.

The PDPA provides for **monetary penalties** in case of non-compliance.

Differences

Depending on the violation that has occurred the penalty may be up to either: **2% of global annual turnover or €10 million**, whichever is higher; or **4% of global annual turnover or €20 million**, whichever is higher. The amount of the penalty may also vary depending on 'the nature, gravity and duration of the infringement,' the nature of the processing, the number of data subjects affected and the damages suffered, the negligent or intentional character of the infringement, etc. (A complete list can be found in Article 83(2) of the GDPR.)

Under the PDPA, the maximum penalty for non-compliance under Sections 26-28 is a fine not exceeding **THB 5 million** (approx. €149,000) can be issued by the expert committee.

Although the GDPR **does not** contain specific provisions outlining criminal penalties for non-compliance, Member States may issue national rules relating to criminal penalties.

Depending on the violation that has occurred under Sections 26-28 of the PDPA, the penalty may be **imprisonment for a term not exceeding one year**.

6.2. Supervisory Authority

Fairly Inconsistent

Both the GDPR and the PDPA provide supervisory authorities with investigatory powers and corrective powers. However, there are differences in the scope of each power under the two laws.

GDPR	PDPA
Articles 51-84 Recitals 117-140	Sections 8, 16, 71-76, 90

Similarities

The supervisory authorities have corrective **powers** which include the authority to:

- order the data controller or data processor to bring processing operations into **compliance** with the provisions of the GDPR, where appropriate, in a specified manner and within a specified period; and
- to impose a **temporary** or definitive limitation, including a **ban** on processing.

The expert committee(s) has **powers** which include the authority to:

- order data controllers and data processors to **comply** with their obligations under the PDPA within the prescribed period; and
- **suppress** data controllers and data processors from performing any activity that causes damage to data subjects within the **prescribed period**.

The supervisory authorities have investigatory **powers** which include the authority to:

- order the data controller and the data processor to **provide any information required** for the performance of its tasks; and
- obtain **access to any premises** of the data controller and the data processor, including to any **data processing equipment** and means, in accordance with European Union or Member State procedural law.

The expert committee(s) designated by the PDPC have **powers** which include the authority to:

- request documents or information related to data protection under the PDPA, which includes issuing a summons to a relevant individual to **provide the required information**; and
- file a complaint to the competent court to issue an order granting permission to the competent officer to **enter the premises** of the data controller, or any person involved in the offence, to investigate and collect facts, and seize documents, evidence, or **any other items** related to the offence.

The supervisory authorities also have a wide range of corrective powers which include the authority to issue **warnings** and **reprimands**, order the rectification or erasure of personal data, and impose **administrative fines**.

The PDPA provides that the expert committee(s) may issue a **warning** before issuing a fine, and when determining whether to issue an **order** to impose an **administrative fine**, the expert committee shall take into consideration the severity of the circumstances of the offence, the size of the organisation, as well as any other circumstances prescribed by the PDPC.

Differences

The supervisory authorities have investigatory powers which include the authority to carry out data protection **audits**, **review certifications** that have been issued, and **notify** the controller or data processor of an alleged infringement under the GDPR.

The PDPA **does not** expressly provide the expert committee(s) with the authority to carry out data protection **audits**, **review certifications** that have been issued, or to **notify** the controller or data processor of an alleged infringement under the PDPA.

GDPR	PDPA

Differences (cont'd)

GDPR	PDPA
The GDPR explicitly **specifies** that each supervisory authority must **independently** perform its obligations and exercise its powers.	The PDPA **does not** explicitly address whether a regulatory authority must act in complete **independence** when performing their obligations.
Under the GDPR, a supervisory authority that receives a complaint of a personal data breach may seek an amicable settlement with **only** the data controller.	Under the PDPA, the expert committee(s) that receives a complaint of a personal data breach is authorised to settle the dispute of such a breach **between** the data controller or data processor and data subjects, subject to the consent of both parties.
The GDPR **does not** specify the **source of funds** that shall be provided to the supervisory authorities. The source of funds in this regard is left to the Member State's discretion.	The PDPA **specifies** that the **source of funds** for the operation of regulatory authorities shall come from the government and subsidies of national public entities/international public entities/ international governmental organisations, including interests/ revenue generated from regulated authorities' property.

6.3. Civil remedies for individuals

Fairly Inconsistent

Both the GDPR and the PDPA provide data subjects with a lawful right to claim for compensation for any damages incurred from violations by data controllers and data processors under the two pieces of legislation, and allow data subjects to lodge complaints with the relevant supervisory authority or expert committee.

However, the PDPA prescribes a broad scope of compensation for data subjects, while the GDPR does not specifically address such scope in its legislation.

GDPR	PDPA
Articles 79-80, 82 Recitals 131, 146-147, 149	Sections 73, 77-78

Similarities

The GDPR provides individuals with a cause of action to **seek compensation** from a data controller and data processor for a violation of the GDPR.

Data subjects are provided with a right to **claim for compensation** for a failure of a data controller and/or data processor (either intentionally or through negligence) to comply with the PDPA.

Under the GDPR, the data subject has the right to **lodge a complaint** with the supervisory authority. The supervisory authority must inform the data subject of the progress and outcome of his or her complaint.

Under the PDPA, data subjects can **lodge a complaint** relating to personal data protection to the expert committee(s).

The GDPR provides that a data controller or processor shall be **exempt from liability to provide compensation** if it proves that it is not in any way responsible for the event giving rise to the damage.

Under the PDPA, data controllers or data subjects **are not subject to an obligation to provide compensation** where it can be proven that:

- damages were caused by *force majeure*, or by an action of the data subjects themselves; or
- the actions of the data controller or data processor were performed based on legitimate grounds.

Differences

The GDPR **does not** provide a scope of compensation that the data controller and data processor must provide to the affected data subjects. However, the GDPR does provide that a data subject has the right to receive compensation from the data controller or processor for the damage suffered.

A **scope of compensation is provided** under the PDPA, which includes any **expense** that data subjects have incurred for the prevention of damage that is likely to be incurred or to suppress damage that has already been incurred.

GDPR	PDPA

Differences (cont'd)

The GDPR allows Member States to provide for the possibility for data subjects to give a mandate for representation to **a not-for-profit body, association, or organisation** that has as its statutory objective the protection of data subject rights.	The PDPA **does not** contain a provision for data subjects to mandate representation from not-for-profit bodies, associations, or organisations.
The GDPR **does not** specifically outline a maximum amount of compensation that a competent court can increase the amount of compensation up to.	The PDPA provides an authority for a competent court to increase the amount of compensation **up to double actual damages at a court's discretion**, as punitive damages.

BLUMENTHAL RICHTER & SUMET
Attorneys and Legal Counselors

OUR FIRM

Blumenthal Richter & Sumet (BRS) is a full-service independent law firm in Bangkok that helps leading international and domestic companies to expand into new markets, grow their businesses and navigate increasingly complex regulatory frameworks in Thailand and Southeast Asia. For more than 40 years, we have built a reputation for providing international standards of legal service, harnessing insightful local knowledge and operating to the highest degree of integrity at all times.

Our licensed Thai, European and U.S. attorneys are client driven and focused on helping you achieve your goals. Working as a team, we strive to deliver the right outcome and tackle not only your legal issues but the factors affecting your industry. Our experience in the automotive, chemicals, cosmetics, energy, financial, hotel and hospitality, logistics, media and telecommunications as well as real estate sectors gives us the market perspective to understand your needs.

8 Partners 1 Senior Counsel 8 Senior Associates 20 Associates

Established in 1976

PRACTICE AREAS

- Corporate and Commercial / M&A
- Foreign Direct Investment
- Real Estate and Construction
- Dispute Resolution and Litigation
- Intellectual Property
- Tech-Media-Telecoms
- Tax and Customs
- Capital Markets
- Banking and Project Finance
- Energy and Infrastructure
- Regulatory Compliance
- Labour and Employment
- Immigration
- Hospitality
- Bankruptcy and Restructuring

BUSINESS ADVISORY SERVICES

- Market Entry Studies
- Feasibility Assessments
- Sourcing
- Site Selection
- Environmental Impact Assessments
- Research Services
- Audit and Accounting Services
- Senior Management Recruitment

(T) +662-022-1000
(F) +662-636-3377
postoffice@brslawyers.com
www.brslawyers.com

BLUMENTHAL RICHTER & SUMET LTD.
Abdulrahim Place, 31st Floor
990 Rama 4 Road
Bangkok 10500, Thailand

NETWORKS

BRS is the exclusive Thailand representative of INTERLAW, the preferred law firm network for companies doing business internationally. With more than 7,500 attorneys in 150 cities worldwide, INTERLAW is ranked as a Band 1 "Elite Law Firm Network" by *Chambers Global* and provides BRS with access to specialist legal practitioners in every major worldwide jurisdiction. BRS is also the Thailand representative of IR-GLOBAL, one of the largest international professional services networks, for Corporate Law, Foreign Direct Investment, Mergers & Acquisitions, Project Finance, Real Estate and Tech-Media-Telecoms.

AWARDS AND RANKINGS

BRS has been consistently ranked as a leading law firm by the legal profession's foremost independent directories, including *Chambers & Partners* and *The Legal 500*. Individual departments and partners have been recognized year-on-year for their outstanding practices and level of expertise, including Corporate and M&A, Real Estate, Tax and Customs and Tech-Media-Telecoms.

For any inquiries, please contact John P. Formichella at john@brslawyers.com.

(T) +662-022-1000
(F) +662-636-3377
postoffice@brslawyers.com
www.brslawyers.com

BLUMENTHAL RICHTER & SUMET LTD.
Abdulrahim Place, 31st Floor
990 Rama 4 Road
Bangkok 10500, Thailand