Comparing privacy laws:
GDPR v. Singapore's PDPA

OneTrust DataGuidance™
REGULATORY RESEARCH SOFTWARE

RAJAH & TANN ASIA
LAWYERS WHO KNOW ASIA

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), Comparisons 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 program.

Rajah & Tann Asia: A full service legal network spread out over 10 countries in South East Asia and beyond. One unified team, one commitment, one standard – driven by multiple talents. A team that understands local conditions and international standards. A team that is always there, ready when you are. Whenever and wherever you are.

Contributors

OneTrust DataGuidance™: Angela Potter, Keshawna Campbell, Mona Benaissa, Theo Stylianou, Victoria Ashcroft, Alexis Galanis, Angus Young

Rajah & Tann Asia: Lionel Tan and Kendrick Deng

Image production credits:

Cover/p.5/p.51: cnythzl / Signature collection / istockphoto.com
Scale key p6-49: enisaksoy / Signature collection / istockphoto.com
Icon p.12-21: Moto-rama / Essentials collection / istockphoto.com
Icon p.22-23: AlexeyBlogoodf / Essentials collection / istockphoto.com
Icon p.25, 29-37: zak00 / Signature collection / istockphoto.com
Icon p.38-45: AlexeyBlogoodf / Essentials collection / istockphoto.com
Icon p.47-51: cnythzl / 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 2012 (No. 26 of 2012) ('PDPA') was passed on 15 October 2012 and in January 2014 the Do Not Call provisions came into effect, closely followed by the data protection provisions in July 2014. Given the practice of using the Advisory Guidelines on Key Concepts in the PDPA ('the Advisory Guidelines on Key Concepts') and on the PDPA for Selected Topics ('the Advisory Guidelines on Selected Topics') both of which were issued by the Personal Data Protection Commission ('PDPC') to interpret and apply the PDPA, this GDPR comparison guide also refers to relevant Advisory Guidelines provisions.

Both laws are generally comprehensive and set out similar personal and extraterritorial scopes. However, while the GDPR applies to both private and public bodies, the PDPA excludes public agencies and organisations acting on behalf of public agencies from its scope. In addition, the GDPR defines special categories of personal data, whereas the PDPA does not distinguish between specific categories of personal data, or between automated and non-automated means of data processing.

Aside from some differences in terminology, both the GDPR and the PDPA share similar concepts of 'data controller' and 'data processor,' and outline an obligation for organisations to appoint a data protection officer ('DPO'). However, unlike the GDPR, the PDPA does not expressly provide for Data Protection Impact Assessments ('DPIA') to be carried out, though the Advisory Guidelines on Key Concepts recommend DPIA in certain circumstances. Furthermore, the Personal Data Protection (Amendment) Bill 2020, published on 14 May 2020, seeks to introduce a number of key reforms, including mandatory data breach notification and data portability provisions, which would further align the PDPA with the GDPR.

In addition, both pieces of legislation provide for restrictions and exceptions in relation to cross-border transfers of personal data to a third country and international organisations, as well as establishing legal grounds and circumstances where cross-border transfers can be lawfully performed.

Further similarities may be found in the rights individuals are entitled to, for instance both the GDPR and the PDPA require data controllers to inform data subjects about the purpose for which their personal data is collected and processed, provide data subjects with the right to withdraw consent to the processing of their personal data, as well as to access to their personal data. Nonetheless, the PDPA does not provide data subjects with the right to request the erasure or deletion of their personal data.

Both the GDPR and the PDPA provide supervisory authorities with wide-ranging investigatory powers and corrective powers and outline significant monetary penalties in cases of non-compliance. However, the maximum penalty under the GDPR is much higher than under the PDPA.

This guide is aimed at highlighting the similarities and differences between the two pieces of legislation in order to help organisations develop their compliance activities.

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 provisions from the two legislative frameworks, a summary of the comparison, and a detailed analysis of the similarities and differences between the GDPR and the PDPA.

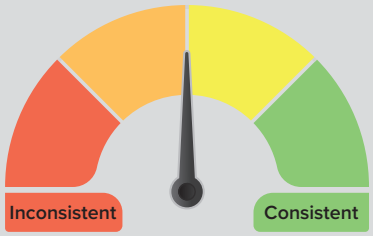
Key for giving the consistency rate

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 the 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 individuals with regard to the use of their personal data, and both utilise concepts that bear some degree of similarity. However, while the GDPR applies to both private and public bodies, the PDPA excludes public agencies and organisations acting on behalf of public agencies from its scope.

GDPR	PDPA
Articles 3, 4(1) Recitals 2, 14, 22-25	Sections 2(1), 4 Personal Data Protection Regulations 2014 ('the Regulations')

Similarities

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 does not apply to personal data about deceased individuals save for provisions relating to **protection** and **disclosure** of personal data, which **would apply** in respect of personal data about an individual who has been **dead for 10 years or fewer**. The PDPA would also **not** apply to personal data about an individual that is contained in a record that **has been in existence for at least 100 years** (even if it is personal data of an individual who is still living).
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.'	Whilst the PDPA does not utilise the concept of a 'data controller', instead using the more general term 'organisations' when defining the entities which are subject to the PDPA's obligations, this term is, with respect to the scope of such obligations, similar to the concept of a '**data controller**' under the GDPR. 'Organisation' is defined in the PDPA as 'any individual, company, association or body of persons, corporate or unincorporated, whether or not (a) formed or recognised under the law of Singapore; or (b) resident, or having an office or a place of business, in Singapore.'
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.'	Whilst the PDPA does not utilise the concept of a 'data processor', the term is similar to the concept of a '**data intermediary**' under the PDPA. 'Data intermediary' is defined in the PDPA as 'an organisation which processes personal data on behalf of another organisation, but does not include an employee of that other organisation.'
Article 4(1) of the GDPR clarifies that a **data subject** is 'an identified or identifiable **natural person**.'	'**Individual**' is defined in the PDPA as 'a **natural person**, whether living or deceased.' Please note that although

GDPR	PDPA

Similarities (cont'd)

	'deceased' is included in this definition, the PDPA explicitly states that it does not apply to personal data about deceased individuals save for the provisions noted above.

Differences

The GDPR **applies** to data controllers and data processors who may be **public bodies**.	The PDPA **does not apply** to any public agencies or organisations acting on behalf of a public agency.
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 the collection, use, and disclosure of personal data of individuals in Singapore and **makes no explicit reference** to their nationality or place of residence in relation to the collection, use, and disclosure of personal data.

1.2. Territorial scope

With regard to extraterritorial scope, the GDPR applies to data controllers and data processors that do not have a presence in the EU but have processing activities that take place in the EU. Similarly, the PDPA applies to all organisations which are not a public agency or acting on behalf of a public agency that carry out activities relating to the collection, use, and disclosure of personal data in Singapore, whether or not they are formed or recognised under the laws of Singapore, or resident or have an office or a place of business in Singapore.

GDPR	PDPA
Articles 3, 4, 11 Recitals 2, 14, 22-25	Section 2(1) Advisory Guidelines on Key Concepts

Similarities

GDPR	PDPA
The GDPR **applies** to organisations that have presence in the EU. In particular, under Article 3, the GDPR applies to entities or organisations that have an '**establishment**' in the EU or if processing of personal data takes place in the context of the activities of that establishment, irrespective of whether the data processing takes place in the EU or not.	The PDPA applies to **all organisations** that carry out activities relating to the collection, use, and disclosure of personal data in Singapore, and are not a public agency or acting on behalf of a public agency
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**.	The PDPA applies to organisations collecting, using, and disclosing personal data in Singapore, **whether or not formed or recognised under the laws of Singapore, or resident or having an office or a place of business in Singapore**.

Differences

GDPR	PDPA
Not applicable.	Not applicable.

1.3. Material scope

Both the GDPR and the PDPA generally define personal data as information that directly or indirectly relates to an individual. Similarly, both laws provide exceptions for personal data processing that is for legal purposes, for personal use, and for certain artistic or media related purposes.

However, the GDPR and the PDPA vary regarding other aspects of material scope. Whilst the GDPR defines special categories of personal data, the PDPA does not distinguish between specific categories of personal data. In addition, unlike the GDPR, the PDPA does not differentiate between automated and non-automated means of data processing.

GDPR	PDPA
Articles 2-4, 9, 26 Recitals 15-21, 26	Sections 2(1), 4(1) Second, Third, and Fourth Schedule Advisory Guidelines on Selected Topics

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, and disclosure** of personal data.

The GDPR defines '**personal data**' as 'any information' that directly or indirectly relates to an identified or identifiable individual.

The PDPA defines '**personal data**' as 'data, whether true or not, about an individual who can be identified (a) from that data; or (b) from that data and other information to which the organisation has or is likely to have access.'

The GDPR **excludes** from its application the processing of personal data by individuals for **purely personal or household purposes**. This is data processing that has 'no connection to a professional or commercial activity.'

The PDPA explicitly **excludes** the application of the data protection provisions to **any individual acting in a personal or domestic capacity, as well as any employee acting in the course of his/her employment with an organisation**.

The GDPR **excludes** from its application data processing in the context of **law enforcement or national security**.

The PDPA **excludes** from its application **public agencies or organisations acting on behalf of a public agency** in relation to the collection, use, or disclosure of personal data. Under the PDPA, 'public agency' includes:

- the Government, including any ministry, department, agency, or organ of the State;

GDPR	PDPA

Similarities (cont'd)

	• any tribunal appointed under any written law; or • any statutory body specified as such by the Minister by notification in the Gazette
The GDPR provides requirements for specific processing situations including processing for **journalistic purposes and academic, artistic or literary expression**.	The PDPA provides exceptions to the need for consent in certain situations, such as the **use or disclosure** of personal data for **research purposes**, and the **collection** of personal data for **artistic or literary purposes, as well as certain journalistic purposes**.
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.	The PDPA **does not define anonymised data**. However, the PDPC's Advisory Guidelines on Selected Topics state that data that has been **anonymised** is **not personal data**, and the data protection provisions in the PDPA would not apply to the collection, use, or disclosure of anonymised data. The Advisory Guidelines on Selected Topics state that 'anonymisation' is the process of converting personal data into data that cannot be used to identify any particular individual.

Differences

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 the processing of special categories of personal data.	Whilst the PDPA **neither distinguishes nor defines special categories of personal data**, based on past decisions by the PDPC, certain types of personal data have been considered to be more sensitive, and organisations that collect, use, or disclose such data would generally be expected to provide more robust standards of protection. Such types of data include **medical data, financial data, bankruptcy status, drug problems and infidelity, personal data of children and personal identifiers (e.g. National Registration Identity Card ('NRIC') and passport details)**.
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 of personal data.

2. Key definitions

2.1. Personal data

Both the GDPR and the PDPA define 'personal data', although the GDPR provides a more detailed definition. While the GDPR also defines sensitive data, the PDPA neither defines nor distinguishes special categories of personal data.

GDPR	PDPA
Articles 4(1), 9 Recitals 26-30	Section 2(1) Advisory Guidelines on Selected Topics

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 'data, whether true or not, about an individual who can be identified (a) from that data; or (b) from that data and other information to which the organisation has or is likely to have access.'

The GDPR **does not** apply to 'anonymised' data, where the data can no longer be used to identify the data subject.

The PDPA **does not** apply to 'anonymised' data, where the data can no longer be used to identify the data subject.

The GDPR specifies that **online identifiers** may be considered as personal data, such as **IP addresses, cookie identifiers, and radio frequency identification tags**.

The PDPC's Advisory Guidelines on Selected Topics state that **online identifiers** such as IP addresses, cookie identifiers, and radio frequency identification tags may be considered as personal data if they can identify individuals.

Differences

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.'

Whilst the PDPA **neither distinguishes nor defines special categories of personal data**, based on past PDPC decisions, certain types of personal data have been considered **more sensitive data**, and organisations that collect, use, or disclose such data would generally be expected to provide more robust standards of protection. Such types of data include **medical data, financial data, bankruptcy status, drug problems and infidelity, personal data of children and personal identifiers (e.g. NRIC and passport details)**.

2.2. Pseudonymisation

The GDPR provides a definition for pseudonymised data and clarifies that such data is subject to the obligations of the GDPR. Unlike the GDPR, the PDPA does not provide a definition of pseudonymised data.

GDPR	PDPA
Articles 4(5), 11 Recitals 26, 29	Not applicable

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

Save for some differences in terminology, both the GDPR and the PDPA share similar concepts of 'data controller' and 'data processor.' There are also common obligations under both laws, such as the requirement to appoint a DPO.

While the GDPR specifically provides that a data controller or data processor must conduct DPIAs in certain circumstances, the PDPA does not expressly provide for DPIAs.

GDPR	PDPA
Articles 4, 17, 28, 30, 32, 33, 35, 37, 38 Recitals 64, 90, 93	Sections 2(1), 4, 26(1) PDPC's Guide to Handling Access Requests (9 Jun 2016) PDPC's Guide to DPIAs (1 November 2017) PDPC's Guide to Managing Data Breaches 2.0 (22 May 2019)

Similarities

The GDPR defines a **data controller** as 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.

Whilst the PDPA does not utilise the term 'data controller,' instead using the more general term 'organisations' when defining the entities which are subject to the PDPA's obligations, the concept of 'organisations', with respect to the scope of such obligations, is similar to the concept of a '**data controller**' under the GDPR. 'Organisation' is defined in the PDPA as 'any individual, company, association or body of persons, corporate or unincorporated, whether or not (a) formed or recognised under the law of Singapore; or (b) resident, or having an office or a place of business, in Singapore.'

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**.

Whilst the PDPA does not utilise the term 'data processor', the concept is similar to that of a '**data intermediary**' under the PDPA. 'Data intermediary' is defined in the PDPA as 'an organisation which **processes personal data on behalf of another organisation**, but does not include an employee of that other organisation.'

Under the GDPR, 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**.

Organisations must comply with the **nine data protection provisions** of the PDPA as set out in Parts III to VI of the PDPA. The nine data protection provisions are as follows:

- Consent Obligation;
- Purpose Limitation Obligation;
- Notification Obligation;
- Access and Correction Obligation;

GDPR	PDPA
Similarities (cont'd)	
	• Accuracy Obligation; • Protection Obligation; • Retention Limitation Obligation; • Transfer Limitation Obligation; and • Accountability Obligation. However, **data intermediaries** are only required to comply with the **Protection Obligation and Retention Limitation Obligation**.
Under the GDPR, data controllers must implement **technical and organisational security measures**.	Organisations must implement **reasonable technical and security measures** to comply with the Protection Obligation of the PDPA.
The GDPR provides for the designation of a **DPO** by data controllers or data processors.	Under the PDPA, all organisations are required to appoint a **DPO**, whose business contact information must be made publicly available. Although the DPO is not required to be physically present in Singapore, they should be readily reachable from Singapore and operational during Singapore business hours.
The GDPR provides that where processing is 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 an **organisation** will have the **same obligations** in respect of personal data **processed on its behalf and for its purposes by a data intermediary as if the personal data were processed by the organisation itself**. Additionally, if the data intermediary is **located overseas** (i.e. outside Singapore), the **Transfer Limitation Obligation** would apply, requiring the organisation to ensure that the (recipient) data intermediary is **bound by legally enforceable obligations** (such as a contract) to provide **a standard of protection that is comparable to that under the PDPA**.
Differences	
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.	The PDPA **does not** contain an equivalent provision.
The GDPR provides that a data controller or data processors conduct **DPIAs** in certain circumstances.	The PDPA does not expressly provide for DPIAs. However, the PDPC has **encouraged organisations to conduct DPIAs** when the

GDPR	PDPA
Differences (cont'd)	
	organisation's system or process is (a) new and in the process of being designed; or (b) in the process of undergoing major changes.
Data controllers must notify supervisory authorities of **data breaches**.	There is currently **no mandatory obligation to notify the PDPC** and/or affected individuals of data breaches. However, the PDPC has announced its intention to introduce a mandatory data breach notification regime as part of proposed future amendments to the PDPA. Although non-binding in nature, the PDPC's Guide to Managing Data Breaches 2.0, issued on 22 May 2019, provides guidelines as to when an organisation is required to notify the PDPC and/or affected individuals about a data breach, and will likely form the framework that will be introduced by the PDPC as part of the mandatory data breach notification regime.
The GDPR stipulates that data controllers and data processors keep **records of processing activities** and provides an exception from this obligation for small organisations.	The PDPA **does not** specifically require organisations to keep records of processing activities. However, the PDPC has indicated that organisations should keep a record of all access requests received and processed, documenting clearly whether the requested access was provided or rejected, as proper documentation may help an organisation in the event of a dispute or an application to the PDPC for a review.

2.4. Children

Unlike the GDPR, the PDPA does not contain provisions specifically targeted at protecting children's personal data. Nonetheless, the PDPC recognises that there is generally greater sensitivity surrounding the treatment of minors and generally expects organisations that collect, use, or disclose personal data of minors to provide more robust standards of protection when collecting, using, or disclosing personal data of minors.

GDPR	PDPA
Articles 6, 8, 12, 40, 57 Recitals 38, 58, 75	Advisory Guidelines on Selected Topics

Similarities

The GDPR **does not** define 'child' nor 'children.'

The PDPA **does not** define 'child' nor 'children.'

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.

As a **general rule**, organisations obtaining personal data from third-party sources should exercise the **appropriate due diligence to check and ensure** that the third-party source can **validly give consent** for the collection, use, and disclosure of personal data on behalf of the individual. This would similarly apply to the situation of obtaining consent from a parent or guardian on behalf of a minor.

Differences

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**.

The PDPA **does not** specify the situations in which a minor (that is, an individual who is less than **21 years of age**) may give consent for the purposes of the PDPA. However, the PDPC's Advisory Guidelines on Selected Topics state that the PDPC will adopt the practical rule of thumb that **a minor who is at least 13 years of age** would typically have sufficient understanding to be **able to consent on his/her own behalf**. The Advisory Guidelines on Selected Topics also state that as a general guide, where the minor is under the age of 13 years, organisations may wish to obtain consent for the collection, use, and disclosure of the minor's personal data from an **individual that can legally give consent on behalf of the minor**, such as the minor's **parent or guardian**.

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** contain provisions that specifically address the collection, use, or disclosure of personal data about minors. However, the PDPC has expressed that given that there is generally greater sensitivity surrounding the treatment of minors, it may be prudent

GDPR	PDPA
Differences (cont'd)	
	for organisations to introduce relevant precautions when collecting, using, or disclosing personal data about minors.
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.	Whilst the PDPA **does not** contain provisions that specifically address the collection, use, or disclosure of personal data about minors, the PDPC has expressed that when information is addressed specifically to a minor, the information should be stated in language that is easily understandable by minors. Organisations should also consider the use of pictures and other visual aids to make such information easier to understand.
The GDPR's provisions on the applicable conditions for the processing children's data apply in respect of **information society services**.	The conditions for processing minors' data identified in PDPC's Advisory Guidelines on Selected Topics appear to be **wider** in scope than the GDPR and apply to the collection, use, or disclosure of personal data in Singapore.

2.5. Research

Fairly inconsistent

Under the GDPR, the processing of sensitive data is not prohibited where necessary for research purposes and when specific measures have been taken to safeguard the fundamental rights and interests of the data subjects. Similarly, under the PDPA, an organisation may collect, use, or disclose personal data for research purposes if individuals have been informed that their personal data will be collected, used, or disclosed for research purposes and their consent has been obtained for the same, unless an exception under the PDPA applies.

Unlike the GDPR, the PDPA does not provide data subjects with the right to object to the processing of their personal data. 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, 159-161	Third Schedule

Similarities

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.).

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.'

Organisations that wish to conduct **analytics and research activities** that require the collection, use, or disclosure of personal data have to comply with the PDPA. In particular, under the PDPA, individuals have to be notified that their personal data will be collected, used, or disclosed for the purpose of analytics and research activities, and their consent must have been obtained for the same, unless an exception under the PDPA applies.

Under paragraph 1(i) of the Third Schedule to the PDPA, organisations may **use personal data without consent** for a research purpose, including historical or statistical research, if all the conditions referred to in paragraph 2 of the Third Schedule are fulfilled. Paragraph 2 states that paragraph 1(i) shall not apply unless:

- the research purpose cannot reasonably be accomplished unless the personal data is provided in an individually identifiable form;
- it is impracticable for the organisation to seek the consent of the individual for the use;
- the personal data will not be used to contact persons to ask them to participate in the research; and
- linkage of the personal data to other information is not harmful to the individuals identified by the personal data and the benefits to be derived from the linkage are clearly in the public interest.

GDPR	PDPA

Similarities (cont'd)

Under the GDPR, data subjects have the **right to object** to the processing of personal data for research purposes **unless such research purposes are for reasons of public interest**.	The PDPA does not provide individuals with the right to object to the processing of their personal data. Nonetheless, under the PDPA, a data subject has the right to **withdraw consent** that was previously given in relation to the collection, use, or disclosure of personal data for analytics and research activities.

Differences

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** provide for the capacity to derogate from data subject rights in relation to processing for research purposes (see the Third Schedule of the PDPA above for exceptions from consent requirement).

3. Legal basis

The GDPR provides a list of legal bases for the processing of personal data and special categories of personal data. Whilst the PDPA does not distinguish specific categories of personal data, it does deem the consent of the individual as central and necessary before commencing data processing activities. Furthermore, both pieces of legislation stipulate that data processing can be carried out by a data controller or organisation if it is required under a legal obligation.

GDPR	PDPA
Articles 5-10 Recitals 39-48	Section 13

Similarities

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 Section 13 of the PDPA, an organisation cannot collect, use, or disclose personal data about an individual unless the individual gives, or is deemed to have given, his/her **consent** to the collection, use, or disclosure. Under the PDPA, an individual has not given consent unless the individual has been notified of the purposes for which his/her personal data will be collected, used, or disclosed, and the individual has provided his consent for those purposes.

Differences

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 PDPA **does not** explicitly outline legal bases for personal data processing, although it does provide that the collection, use, or disclosure can be done without the consent of the individual only if it **is required or authorised under the PDPA or any other written law** (see the Second, Third, and Fourth Schedules of the PDPA).

GDPR	PDPA

Difference (cont'd)

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 **neither** distinguishes nor defines special categories of personal data.

4. Controller and processor obligations

4.1. Data transfers

Fairly inconsistent

Both the GDPR and the PDPA provide for restrictions and exceptions in relation to cross-border transfers of personal data to a third country and international organisations. In addition, both outline legal grounds and circumstances where cross-border transfers can be lawfully performed.

However, unlike the PDPA, the GDPR provides for cross-border transfers made from a register, and allows cross-border transfers carried out under international agreements for judicial cooperation.

GDPR	PDPA
Articles 44-50 Recitals 101, 112	Section 26 Advisory Guidelines on Key Concepts The Regulations

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.

The PDPA provides that an organisation must not transfer personal data to a country or territory outside Singapore except in accordance with requirements prescribed under the PDPA, including legally enforceable obligations, to ensure that organisations provide a standard of protection to transferred personal data that is **comparable to the standard of protection provided under the PDPA**, unless written exemption from the PDPC is obtained.

Differences

Under the GDPR, one of the following **legal grounds** must be established for the transfer of personal data abroad:

- **prior consent;**
- 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.

An organisation will be recognised as having taken appropriate steps to ensure that the recipient of transferred personal data is bound by legally enforceable obligations to provide a standard of protection that is comparable to that under the PDPA if:

- subject to conditions, the individual whose personal data is to be transferred gives his/her **consent** to the transfer of his personal data;
- the transfer is necessary for the performance of a **contract** between the **organisation** and the **individual**, or to do anything at the individual's request with a view to his entering a contract with the organisation;
- the transfer is necessary for the conclusion or performance of a **contract** between the **organisation** and **a third party** which is entered into at the individual's request, or which a reasonable person would consider to be in the individual's interest;

Differences (cont'd)

- the transfer is necessary for a use or disclosure in certain **situations where the consent of the individual is not required** under the PDPA. In such cases, the organisation may only transfer personal data if it has taken **reasonable steps** to ensure that the personal data will not be used or disclosed by the recipient for any other purpose;
- the personal data is **data in transit**; or
- the personal data **is publicly available** in Singapore.

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 ('BCR') with specific requirements (e.g. a legal basis for processing, a retention period, complaint procedures, etc.);
- Standard Contractual Clauses ('SCC') adopted by the EU Commission or by a supervisory authority;
- an approved code of conduct; or
- an approved certification mechanism.

The PDPA **does not** contain a similar provision. However, the Advisory Guidelines on Key Concepts provide that the following may be used to demonstrate that the recipient is bound by legally enforceable obligations to provide to the personal data transferred a standard of protection that is comparable to that under the PDPA, as required under Section 26 of the PDPA:

- any law;
- BCR that:
  - require recipients of transferred personal data to provide a standard of protection that is at least comparable to the protection under the PDPA; and
  - specify the recipients of the transferred personal data to which the BCR apply; the countries and territories to which the personal data may be transferred under the BCR; and the rights and obligations provided by the BCR;
- a contract that requires the recipient to provide to the transferred data a standard of protection that is at least comparable to the standard of protection under the PDPA; and
- specifies the countries and territories to which the personal data may be transferred under the contract; or
- any other legally binding instrument.

In addition, the Advisory Guidelines on Key Topics provide that if the recipient organisation holds a 'specified certification' that is granted or recognised under the law of that country or territory to which the personal data is transferred, the recipient organisation is taken to be bound by such legally enforceable obligations. Under the Data Protection Regulations 2014, 'specified certification' refers to certifications under the Asia Pacific Economic Cooperation Cross Border Privacy Rules ('APEC CBPR') System, and the Asia Pacific Economic Cooperation Privacy Recognition for Processors ('PRP') System.

GDPR	PDPA
The GDPR specifies that a cross-border transfer is allowed based on **international agreements** for judicial cooperation.	The PDPA **does not** specify whether cross-border transfers based on international agreements for judicial cooperation are permitted.
The grounds for a cross-border **transfer includes the transfer being made from a register** which, according to the Union or a Member State 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** establish a similar provision.

4.2. Data processing records

The GDPR imposes an obligation on data controllers, their representatives, and data processors to maintain a record of processing activities, and outlines specific information that must be included within the record. The PDPA does not impose any obligations relating to recordkeeping of data processing activities.

GDPR	PDPA
Article 30 Recital 82	Advisory Guidelines on Key Concepts

Similarities

GDPR	PDPA
Not applicable.	Not applicable.

Differences

Under the GDPR, data controllers and data processors have an obligation to **maintain a record** of processing activities under their responsibility. In addition, 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 GDPR also prescribes a similar list for data processors, requires that records be maintained in **writing or electronic form**, and details exceptions **organisations 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.

The PDPA does **not** impose an obligation on organisations to maintain a record of processing activities. However, the PDPC has indicated in its Advisory Guidelines on Key Concepts that organisations should **keep a record of all access requests received and processed, documenting clearly whether the requested access was provided or rejected**, as proper documentation may help an organisation in the event of a dispute or an application to the PDPC for a review.

4.3. Data processing impact assessment

Unlike the GDPR, the PDPA does not contain any provisions addressing DPIAs. However, the PDPC's Guide to Data Protection Impact Assessments (1 November 2017) highlights that organisations may wish to conduct a DPIA in certain circumstances in order to ensure that their handling of personal data is compliant with the requirements of the PDPA.

GDPR	PDPA
Articles 35, 36 Recitals 75, 84, 89-93	PDPC's Guide to DPIAs (1 November 2017)

Similarities

GDPR	PDPA
Not applicable.	Not applicable.

Differences

GDPR	PDPA
The GDPR provides that a DPIA must be conducted **under the following circumstances**: • if a data controller utilises **new technologies** to process personal data; • 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 • there is systematic monitoring of a publicly accessible area on a large scale. In addition, the GDPR specifies requirements for **further reviews** and obligations for **prior consultation** with a supervisory authority. The GDPR also outlines that an 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 PDPA **does not** contain a similar requirement. However, in the PDPC's Guide to DPIAs (1 November 2017), the PDPC has encouraged organisations to conduct DPIAs when the organisation's system or process is (a) new and in the process of being designed or (b) in the process of undergoing major changes.

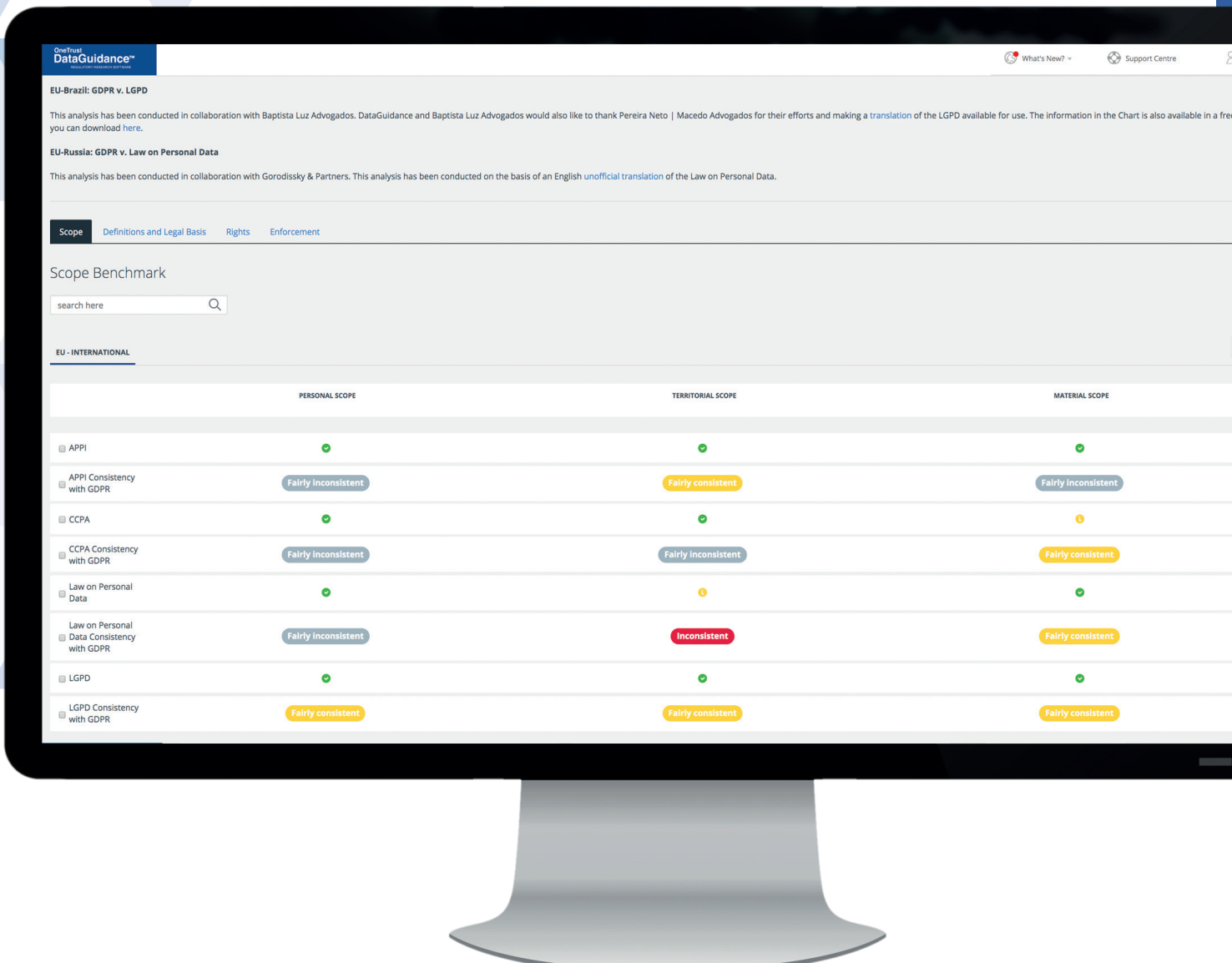
OneTrust DataGuidance™

REGULATORY RESEARCH SOFTWARE

Global Regulatory Research Software

40 In-House Legal Researchers, 500 Lawyers
Across 300 Jurisdictions

Monitor regulatory developments, mitigate risk
and achieve global compliance.

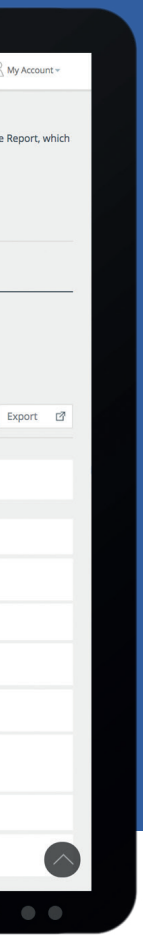


Build a global privacy program by comparing key legal frameworks against the GDPR

CCPA | Russia | Thailand | Brazil | Japan

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

The GDPR Benchmarking tool provides a comparison of the various pieces of legislation on the following key provisions.



- Scope
- Rights
- Definitions and legal basis
- Enforcement

- Employ topic specific guidance to develop your compliance activities
- Monitor news and access written opinion pieces on the most recent developments

Start your **free trial** today at **dataguidance.com**

4.4. Data protection officer appointment

Both the GDPR and the PDPA provide for the appointment of a data protection officer ('DPO'). However, unlike the GDPR, the PDPA does not provide a definition of a DPO. In addition, the GDPR details the independence and professional qualities as well as expertise necessary to be appointed as a DPO, whereas the PDPA does not. Finally, the PDPA allows for more than one DPO to be appointed, whereas the GDPR does not address this matter.

GDPR	PDPA
Articles 13-14, 37-39 Recital 97	Section 11(3)

Similarities

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

Under the PDPA, an organisation shall **designate** one or more individuals to be responsible for ensuring that the organisation complies with the PDPA.

Under the GDPR, a DPO's tasks include:

- **informing and advising** 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;
- **monitoring 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
- **acting 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.

Under the PDPA, the possible responsibilities of the DPO may include, but are not limited to, the following:

- **ensuring compliance** with the PDPA when developing and implementing policies and processes for handling personal data;
- **fostering a data protection culture** among employees by communicating personal data protection policies to stakeholders and conducting training sessions for employees to familiarise them with the company's data protection policies and guidelines;
- managing personal data protection related **queries and complaints**;
- **alerting management** to any risks that might arise with regard to personal data; and
- **liaising with the PDPC** on data protection matters, if necessary.

The **contact details** of the DPO must be included in the privacy notice for data subjects and communicated to the supervisory authority.

An organisation must make available to the public the **business contact information** of at least one of the individuals designated.

Differences

Under the GDPR, data controllers and data processors are only required to designate a DPO 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

All organisations are required to appoint a DPO.

GDPR	PDPA

Differences (cont'd)

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

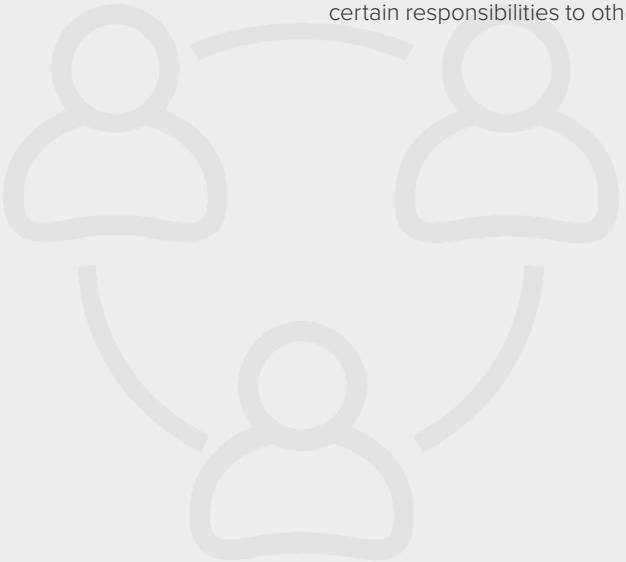
- the core activities of the controller or the processor relate to a large scale of **special categories of personal data** (e.g. religious beliefs, ethnic origin, data required for the establishment, exercise, or defence of legal claims etc.)

The GDPR provides that a group may appoint a **single DPO** who must be easily contactable by each establishment, that the DPO shall be designated on the basis of **professional qualities and expert knowledge** of data protection law and practices, and that data subjects **may contact** the DPO with regard to the processing of their personal data as well as the exercising of their rights. The GDPR also recognises the **independence** of DPOs and ensures that DPOs are **provided with the resources necessary** to carry out his or her obligations. The GDPR specifies that the DPO can be a **staff member** of the data controller or data processor or can perform tasks based on a **service contract**.

The PDPA **does not** contain equivalent provisions regarding the appointment and role of a DPO.

The GDPR **does not** explicitly refer to DPO teams or the delegation of DPO responsibilities.

The PDPA provides that an organisation may appoint **one person or a team of persons** to be its DPO. Once appointed, the DPO may in turn delegate certain responsibilities to other officers.



4.5. Data security and data breaches

Fairly inconsistent

Both the GDPR and the PDPA outline requirements in relation to implementing security arrangements and various technical measures. However, the GDPR includes an obligation to notify the relevant authorities, as well as the impacted data subjects, of data breaches in certain circumstances within a set timeline, whereas presently, there is no requirement for organisations to notify any party when a data breach has occurred under the PDPA.

However, the PDPC has announced its intention to introduce a mandatory breach notification regime as part of future proposed amendments to the PDPA. Under the draft Personal Data Protection (Amendment) Bill, organisations will be required to notify the PDPC of a data breach that results in, or is likely to result in, significant harm to the individuals to whom any personal data affected by a data breach relates to or is of a significant scale. Organisations will also be required to notify the affected individuals if the data breach is likely to result in significant harm to them.

GDPR	PDPA
Article 5, 24, 32-34 Recitals 74-77, 83-88	Section 24 Advisory Guidelines on Key Concepts

Similarities

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 an organisation shall protect personal data in its possession or under its control by making reasonable **security arrangements** to prevent unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks.

The GDPR provides a **list** of **technical and organisational measures**, where appropriate, that data controllers and data processors may 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.

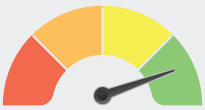
The Advisory Guidelines on Key Concepts provide a **list** of example **technical measures** that organisations could implement, such as encrypting personal data, adopting appropriate access controls, and ensuring computer networks are secure.

Differences

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. The controller must also **notify relevant data subjects** 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, unless certain exceptions apply. The GDPR also specifies information such notifications must contain. In addition, the GDPR provides that 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, and stipulates that **data processors must notify** the data controller without **undue delay** after becoming aware of the personal data breach.

The PDPA presently **does not** contain a similar data breach notification requirement.

4.6. Accountability



Both the GDPR and the PDPA recognise an organisation's accountability for personal data in its possession or under its control as a fundamental privacy principle. Furthermore, both pieces of legislation contain provisions that can be taken to apply to accountability, such as the requirement to designate a DPO.

GDPR	PDPA
Article 5, 24-25, 35, 37 Recital 39	Section 11(2)

Similarities

GDPR	PDPA
The GDPR recognises **accountability** as a fundamental principle of data protection. In particular, Article 5(2) of the GDPR states that 'the data controller shall be responsible and able to demonstrate compliance with the data protection principles provided for under Article 5(1). In addition, the accountability principle can be taken to apply to several other requirements, as mentioned in other sections of this report, including the appointment of a DPO, and DPIAs.	The PDPA recognises the **Accountability Obligation** (previously known as the Openness Obligation) as a fundamental principle of data protection. The Accountability Obligation is premised on Section 11(2) of the PDPA which states that 'an organisation is responsible for personal data in its possession or under its control.' Furthermore, accountability can be taken to apply to other requirements, including the appointment of a DPO and the requirement for an organisation to develop and implement data protection policies and practices to meet its obligations under the PDPA.

Differences

GDPR	PDPA
Not applicable.	Not applicable.

5. Individuals' rights

5.1. Right to erasure

Unlike the GDPR, the PDPA does not provide data subjects with the right to request the erasure or deletion of their personal data. Under the PDPA, there are only general requirements in relation to ceasing to retain data once the purpose for which the personal data was collected is no longer being served by retention of the personal data, and retention is no longer necessary for legal or business purposes.

GDPR	PDPA
Articles 12, 17 Recitals 59, 65-66	Sections 16, 25 Advisory Guidelines on Key Concepts

Similarities

GDPR	PDPA
Not applicable.	Not applicable.

Differences

Under the GDPR, the right to erasure applies if certain grounds apply, 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 GDPR further specifies that this right can be exercised **free of charge**, data subjects **must be informed** that they have the right to request for their data to be deleted, and that responses must be made within **one month** with the potential for extending this deadline for two additional months. The GDPR also specifies related exceptions and format requirements.

The PDPA **does not** provide data subjects with the right to erasure. The Advisory Guidelines on Key Concepts clarify that an individual may withdraw consent for the collection, use, or disclosure of his personal data, but the PDPA does not require an organisation to delete or destroy the individual's personal data upon request and may retain it for as long as there are business or legal needs.

5.2. Right to be informed

Fairly inconsistent

The GDPR and the PDPA both require data controllers to inform data subjects about the purpose for which their personal data is collected and processed. In addition, both pieces of legislation require data controllers and organisations to disclose business contact information of the DPO to respond to data subjects' queries.

However, the GDPR requires data controllers to inform data subjects of the potential consequences of the processing of personal data, and stipulates that information must be sent in written form to the data subjects, whereas the PDPA does not specify the means by which information must be shared.

GDPR	PDPA
Articles 5-14 Recitals 58 - 63	Section 20 Advisory Guidelines on Key Concepts

Similarities

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

- **purposes** of processing, including the legal basis for processing; and
- **contact details** of the data controller or its representative and the DPO.

An organisation must inform the individual of:

- the **purposes** for the collection, use, and/or disclosure of the personal data, as the case may be, on or before collecting the personal data; and
- on request by the individual, the **business contact information** of a person who is able to answer on behalf of the organisation the individual's questions about the collection, use, or disclosure of the personal data.

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**.

Under the PDPA, an organisation **must inform the data subject of any other purpose** for which the data collected will be used or disclosed.

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**.

Information relating to personal data processing (e.g. the purpose of the collection, use, or disclosure) must be provided to the data subjects **on or before collecting, using, or processing such personal data**.

Differences

Under the GDPR data subjects must be provided with the following information relating to the processing of personal:

- **details of personal data** to be processed;
- **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**; and
- r**ecipients or their categories** of personal data.

The PDPA **does not** explicitly require organisations to provide this information. However, an organisation should state its purposes at an appropriate level of detail for the individual to determine the reasons and manner in which the organisation will be collecting, using, or disclosing his personal data.

GDPR	PDPA
Differences (Cont'd)	
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.	The PDPA **does not** contain a similar requirement regarding the consequences of failing to provide information.
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 **does not** require organisations to provide information to the data subjects when their personal data has been collected from a third party. However, organisations obtaining personal data from third-party sources should exercise the appropriate due diligence to check and ensure that the third-party source can validly give consent for the collection, use, and disclosure of personal data on behalf of the individual or that the source had obtained consent for disclosure of the personal data.
Information can be provided to data subjects **orally**, in writing, or by electronic means.	The PDPA **does not** specify a manner or form in which an organisation is to inform an individual of the purposes for which it is collecting, using, or disclosing their data. An organisation should determine the best way to ensure that the individual is provided with the required information to understand the purposes for which his personal data is collected, used, or disclosed.
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**.	The PDPA **does not** contain a similar requirement regarding indirect collection.
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** contain a similar requirement regarding automated decision-making.
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.	The PDPA **does not** contain a similar requirement regarding informing data subjects of adequacy decisions.

GDPR	PDPA

Differences (Cont'd)

Information must 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**.

The PDPA **does not** contain a similar provision. However, the Advisory Guidelines on Key Concepts note that it is generally good practice for an organisation to state its purpose in a written form (which may be electronic or other form of documentary evidence) so that the individual is clear about its purpose and both parties will be able to refer to a clearly documented statement of the organisation's purpose in the event of any dispute.

5.3. Right to object

Fairly inconsistent

Both the GDPR and the PDPA provide data subjects and individuals with the right to withdraw consent to the processing of their personal data. However, the GDPR provides data subjects with the right to object to the processing of their personal data, whereas the PDPA does not provide such a right.

GDPR	PDPA
Articles 7, 12, 18, 21	Section 16

Similarities

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

Individuals may, **at any time**, **withdraw** any consent given or deemed to have been given under the PDPA in respect of the collection, use, or disclosure of their personal data for any purpose by an organisation.

Differences

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**.

The data subject has the right to be **informed** about the right to object, and how to exercise this right.

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 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** provide the right to object in a similar manner to that provided in the GDPR.

5.4. Right of access

Both the GDPR and the PDPA provide data subjects with the right to access personal data in the possession of a data controller or organisation, respectively.

However, the GDPR and the PDPA contain notable differences with regard to the implementation of the right to access, including how requests must be communicated and on verifying the identity of the data subject. Furthermore, the GDPR provides detailed guidance on the information that must be included in an access request, whereas the PDPA does not.

GDPR	PDPA
Article 15 Recitals 59-64	Sections 21, 28, Fifth Schedule The Regulations

Similarities

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

The PDPA provides individuals with a **right of access** to personal data about the individual that is in the possession or under the control of an organisation.

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.

An organisation must respond to an access request **as soon as reasonably possible** from the time the access request is received. Furthermore, if an organisation is unable to respond to an access request **within 30 days**, the organisation must instead inform the individual in writing of the time by which it will be able to respond to the request.

A data controller can refuse to act on a request when it is **manifestly unfounded, excessive, or has a repetitive character.**

An organisation is not required to provide access if the burden or expense of providing access would be **unreasonable** to the organisation or **disproportionate** to the individual's interest, or if the request is otherwise **frivolous or vexatious.**

The GDPR provides that the right of access must not adversely affect the rights or freedoms of others, **including those related to trade secrets**.

The PDPA provides that an organisation is not required to provide personal data which, if disclosed, would reveal **confidential commercial information** that could, in the opinion of a reasonable person, harm the competitive position of the organisation.

Differences

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

- the **purposes** of the processing;

Section 21(1) of the PDPA provides that, upon request by an individual, an organisation shall provide the individual with the following as soon as reasonably possible:

- **personal data about the individual** that is in the possession or

GDPR	PDPA

Differences (cont'd)

- 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;
- 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.

under the control of the organisation; and

- information about the **ways in which that personal data has been or may have been used or disclosed** by the organisation within a year before the date of the individual's request.

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 by which data subjects can make an access request. However, the Advisory Guidelines on Key Concepts note that where an individual making the access request asks for a copy of personal data in documentary form, an organisation should provide the copy and have the option of charging the individual a reasonable fee for producing the copy.

The GDPR specifies that a data controller must **have in place mechanisms** for identify verification.

The PDPA **does not** contain a similar provision on identity verification mechanisms.

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.

An organisation **may charge an individual a reasonable fee** to process an access request by the individual.

5.5. Right not to be subject to discrimination

The right not to be subject to discrimination in exercising rights is not explicitly mentioned in the GDPR or the PDPA. However, under the GDPR and the PDPA, the right not to be subject to discrimination can be inferred from the fundamental rights of the data subject.

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 address 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

Presently, the PDPA does not contain any provisions on the right of data subjects to data portability. However, the Personal Data Protection (Amendment) Bill would introduce a data portability obligation similar to the right to data portability under the GDPR, which would require organisations, at the request of the individuals, to share the individual's personal data to another organisation, in a machine-readable format.

GDPR	PDPA
Articles 12, 20, 28 Recital 68, 73	Not applicable

Similarities

GDPR	PDPA
Not applicable.	Not applicable.

Differences

GDPR	PDPA
The GDPR provides individuals with the **right to data portability** and defines the right to data portability as the **right to receive data processed on the basis of contract or consent and processed by automated means, in a 'structured, commonly used, and machine-readable format**' and to transmit that data to another controller without hindrance.	The PDPA **does not** include a right to data portability.

⚠ 6. Enforcement

Fairly inconsistent

6.1. Monetary penalties

Both the GDPR and the PDPA provide for the possible imposition of significant monetary penalties in cases of non-compliance. However, the GDPR's maximum limit for monetary penalties is much higher than that of the PDPA.

GDPR	PDPA
Article 83-84 Recitals 148-149	Section 29 PDPC's Guide on Active Enforcement (21 May 2019)

Similarities

The GDPR provides for the possibility of **administrative, monetary penalties** to be issued by the supervisory authorities in cases of non-compliance.

The PDPA provides for the possibility of **administrative, monetary penalties** to be issued by the PDPC in cases of non-compliance.

When applying an administrative sanction, the supervisory authority must consider: (i) the nature, gravity and duration of the infringement; (ii) the intentional or negligent character of the infringement; (iii) any action taken to mitigate the damage; (iv) the degree of responsibility of the controller or processor; (v) any relevant previous infringements; (vi) the degree of cooperation with the supervisory authority; (vii) the categories of personal data affected by the infringement; (viii) the manner in which the infringement became known to the supervisory authority; (ix) where measures referred to in Article 58(2) have previously been ordered against the controller or processor concerned with regard to the same subject-matter, compliance with those measures; (x) adherence to approved codes of conduct or approved certification mechanisms; and (xi) any other aggravating or mitigating factor applicable to the circumstances of the case.

The PDPC's Guide on Active Enforcement states that **generally, financial penalties are reserved only for breaches** which the PDPC views as particularly **serious in nature**. In assessing the seriousness of the breach, the PDPC considers the following non-exhaustive list of factors: (i) impact of the organisation's breach; (ii) whether the organisation had acted deliberately or wilfully; (iii) whether the organisation had known or ought to have known the risk of a serious contravention and failed to take reasonable steps to prevent it; (iv) extent of non-compliance in terms of the PDPA obligations that the organisation had failed to discharge; (v) number of individuals whose personal data had been subjected to harm and risks as a result of the breach; (vi) whether the organisation had appointed a DPO or equivalent to ensure accountability with the PDPA; (vii) types of personal data that were compromised or put at risk as a result of the breach; and (viii) whether the organisation had previously been found to have similarly breached the PDPA.

Differences

Supervisory authorities may develop guidelines that establish further criteria to **calculate the amount** of the monetary penalty.

The PDPA **does not** include a similar provision. However, the PDPC's Guide on Active Enforcement states that where a financial penalty is warranted, the PDPC would adopt the following principles to determine the amount: (i) the amount should be proportionate to the seriousness of the breach; (ii) the amount should provide sufficient deterrence against future or continued non-compliance by the organisation and others; (iii)

GDPR	PDPA
Differences (cont'd)	
	the amount should take into account aggravating and mitigating factors; (iv) cooperativeness of the organisation in the course of investigations; (v) whether remedial action(s) were implemented; (vi) whether there was voluntary notification of the data breach; (vii) whether the organisation had engaged with the affected individuals in a meaningful manner and had voluntarily offered a remedy, and that the individuals had accepted the remedy; and (viii) whether the organisation admitted to liability for the data breach.
The GDPR provides for the application of fines **to government bodies**. It is, though, left to Member States to create rules on the application of administrative fines to public authorities and bodies.	The PDPA **does not** apply to public authorities and bodies.
Depending on the violation 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.	Depending on the violation, the PDPC may impose a financial penalty of up to **SGD 1 million (approx. €650,000)**.

6.2. Supervisory authorities

Both the GDPR and the PDPA provide supervisory authorities with wide-ranging investigatory powers and corrective powers. The scope of these powers under the two laws is fairly consistent, and the PDPC can be considered a relatively active authority when compared with EU equivalents.

GDPR	PDPA
Articles 51-84 Recitals 117-140	Sections 6, 50 Ninth Schedule

Similarities

GDPR	PDPA
Under the GDPR, supervisory authorities have **investigatory powers** which include: (i) ordering a controller and processor to provide information required; (ii) conducting data protection audits; (iii) carrying out a review of certifications issued; and (iv) obtaining access to all personal data and to any premises.	Under the PDPA, the PDPC has **powers of investigation**, which include requiring an organisation to produce a specified document or specified information which the PDPC or one of its inspectors considers relevant to an investigation. If the document is produced, the PDPC may take copies of it or extracts from it, and require an explanation of the document. If the document is not produced, the PDPC may require an organisation or person to state where it is. The PDPC has the power to enter premises under warrant. The PDPC may also enter into any premises without a warrant by giving the occupier of the premises at least two working days' written notice of the intended entry, and indicating the subject matter and purpose of the investigation.
Under the GDPR, supervisory authorities have **corrective powers** which include: (i) issuing warnings and reprimands; (ii) imposing a temporary or definitive limitation including a ban on processing; (iii) ordering the rectification or erasure of personal; and (iv) imposing administrative fines.	Under the PDPA, the PDPC has the **power to issue the following directions** to an organisation: (i) to stop collecting, using or disclosing personal data in contravention of the PDPA; (ii) to destroy personal data collected in contravention of the PDPA; (iii) to comply with any direction of the PDPC; or (iv) to pay a financial penalty of up to SGD 1 million (approx. €650,000).
Under the GDPR, supervisory authorities shall also: (i) **handle complaints** lodged by data subjects; and (ii) **cooperate** with data protection authorities from other countries.	Under the PDPA, the functions of the PDPC include (i) **handling complaints** lodged by individuals; (ii) **representing the Singapore Government internationally** on matters relating to data protection; and (iii) managing technical **co-operation** and exchange in the area of data protection with foreign data protection authorities and international or inter-governmental organisations.
Under the GDPR, supervisory authorities are tasked with **promoting public awareness** and understanding of the risks,	Under the PDPA, the functions of the PDPC include, among other things, **promoting awareness** of data protection

GDPR	PDPA

Similarities (Cont'd)

rules, safeguards and rights in relation to processing as well as promoting the awareness of controllers and processors of their obligations, amongst other tasks.	in Singapore, conducting research and studies and promoting educational activities relating to data protection, including organising and conducting seminars, workshops and symposia relating thereto, and supporting other organisations conducting such activities.

Differences

It is left to **each Member State to establish a supervisory authority**, and to determine the qualifications required to be a member, and the obligations related to the work, such as duration of term as well as conditions for reappointment.	The **PDPA stipulates that the PDPC shall be responsible** for the administration of the PDPA.
Supervisory authorities may be subject to financial control only if it does not affect its **independence**. They have separate, public annual budgets, which may be part of the overall national budget.	**The PDPC is part of the Info-communications Media Development Authority ('IMDA')**. IMDA receives an annual operating budget from the Ministry of Communications and Information, a ministry of the Government of Singapore.

6.3. Civil remedies for individuals

Both the GDPR and the PDPA provide individuals with a legal right to claim relief for any damages incurred from violations by organisations, and allow for the lodging of complaints with the relevant authority.

GDPR	PDPA
Articles 79, 80, 82 Recitals 131, 146-147, 149	Section 32

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.

The PDPA provides that any person who suffers loss or damage directly as a result of a contravention of any of the data protection provisions in Part IV, V, or VI of the PDPA by an organisation may commence a **private civil action** in respect of such loss or damage suffered.

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.

An individual may **lodge a complaint** relating to personal data protection to the PDPC.

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, **only individuals who have suffered loss or damage directly as a result of a contravention** of any of the data protection provisions in Part IV, V, or VI of the PDPA may commence a private civil action in respect of such loss or damage suffered.

Differences

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 individuals to give a mandate for representation to not-for-profit bodies, associations, or organisations.

RAJAH & TANN ASIA

LAWYERS WHO KNOW ASIA

HERE TO GIVE YOU HOME ADVANTAGE

Where bright minds form one of the largest dedicated Technology, Media & Telecommunications teams in the region.

With unmatched cross-border capabilities, we are the clear market leader in providing a comprehensive suite of data protection services and technology related legal work. Our lawyers are equipped with the expertise and experience to provide incisive legal advice and to embrace the application of existing laws and principles to new offerings.

RAJAH & TANN ASIA

CAMBODIA | CHINA | INDONESIA | LAOS | MALAYSIA | MYANMAR | PHILIPPINES | SINGAPORE | THAILAND | VIETNAM

www.rajahtannasia.com

RAJAH & TANN ASIA

LAWYERS WHO KNOW ASIA

LED BY LEADING LAWYERS, RAJAH & TANN HAS WON NUMEROUS AWARDS AND ACCOLADES FOR EXCELLENCE IN LEGAL SERVICE OVER THE YEARS.

BAND 1 - TMT

"AT THE TOP OF THEIR GAME"

CHAMBERS ASIA PACIFIC 2020

TIER 1 - TMT

"THE 'GO TO' PRACTICE FOR MAJOR CORPORATE CLIENTS ACROSS VARIOUS INDUSTRIES"

THE LEGAL 500 ASIA PACIFIC 2020

OUTSTANDING - TECHNOLOGY & TELECOMMUNICATIONS

ASIALAW PROFILES 2020