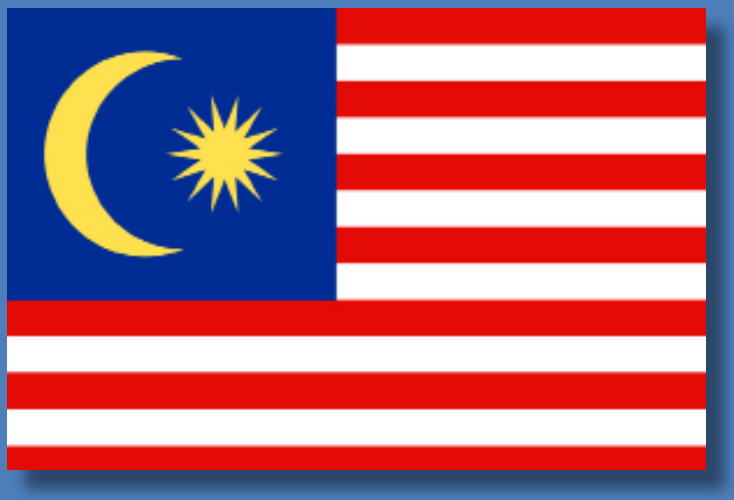


Comparing privacy laws:
GDPR v. Kenya Data Protection PDPA

OneTrust DataGuidance™
REGULATORY RESEARCH SOFTWARE

About the authors

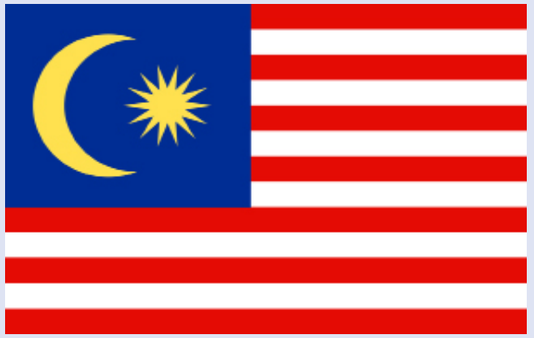
OneTrust DataGuidance™ provides a suite of privacy solutions designed to help organisations monitor regulatory developments, mitigate risk and achieve global compliance.

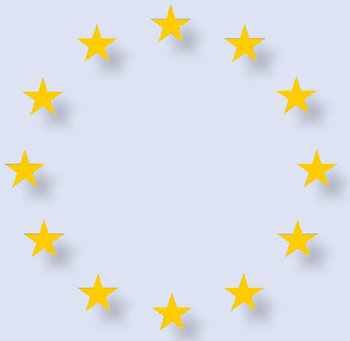
The OneTrust DataGuidance™ platform includes focused guidance around core topics (i.e. GDPR, data transfers, breach notification, among others), Cross-Border Charts which allow you to compare regulations across multiple jurisdictions at a glance, a daily customised news service and expert analysis.

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.

Image production credits:
Cover/p.5/p.51: 221A / Signature collection / istockphoto.com | MicroStockHub / Signature collection / istockphoto.com
Scale key p6-49: enisaksoy / Signature collection / istockphoto.com
Icon p.33-40: AlexeyBlogoodf / Essentials collection / istockphoto.com
Icon p.47-51: cnythzl / Signature collection / istockphoto.com | MicroStockHub / Signature collection / istockphoto.com

Table of contents





Introduction

The General Data Protection Regulation (Regulation (EU) 2016/679) ('GDPR'), which came into effect on 25 May 2018, governs the protection of personal data in European Union and European Economic Area Member States. The Personal Data Protection PDPA 2010 ('PDPA') which took effect on 15 November 2013, and its subsidiary legislation:

- the Personal Data Protection Regulations 2013 ('the Regulations');
- the Personal Data Protection (Class of Data Users) Order 2013 ('the Personal Data Protection Order 2013');
- the Personal Data Protection (Registration of Data User) Regulations 2013;
- the Personal Data Protection (Fees) Regulations 2013 ('Fees Regulation') ('the Fees Regulation');
- the Personal Data Protection (Compounding of Offences) Regulations 2016; and
- the Personal Data Protection (Class of Data Users) (Amendment) Order 2016 ('the Personal Data Protection Order 2016')

are the primary and subsidiary legislation governing the collection and processing of personal data in Malaysia. The Department of Personal Data Protection ('PDP') is the national data protection regulator in the region, and has corrective, advisory, and investigatory powers including the conducting of on-site investigations, issuance of decisions, as well as corrective orders.

In general terms, there are broad similarities between the PDPA and the GDPR. The two legislations contain similar concepts of data controller, data processor, general and sensitive personal data as well as data processing. In addition, the PDPA and the GDPR address matters such as lawful bases for data processing, requirements of record keeping, and data subject rights, although the GDPR provides more wide-ranging and detailed rights to its data subjects in comparison to the PDPA. Nevertheless, the PDPA and the GDPR contain notable differences, including the protection of children, data controller's responsibilities such as the conducting of a Data Protection Impact Assessment ('DPIA'), the appointment of a data protection officer ('DPO'), and the reporting of data breaches to authorities and affected individuals.

This overview organises provisions from the PDPA and the GDPR into key topics and sets them alongside each other to enable analysis and comparison. Each section begins with a detailing of principal information and a general introduction, as well as a consistency rating.

Structure and overview of the Guide

This Guide provides a comparison of the two legislative frameworks 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 legal frameworks, a summary of the comparison, and a detailed analysis of the similarities and differences between the GDPR and the PDPA.

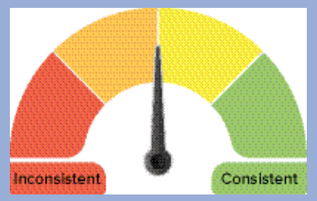
Key for giving the consistency rate

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 informational 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 PDPAed upon without specific legal advice based on particular circumstances.

1. Scope

1.1. Personal scope

Unlike the GDPR, the PDPA does not apply to public bodies. In addition, the PDPA does not specify its applicability based on the nationality of the data subject, nor does it clarify its applicability in relation to deceased individuals, whereas the GDPR provides such information.

GDPR	PDPA
Data controller	
Article 4(7): 'controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.	Section 4(21): 'data user' means a person who either alone or jointly or in common with other persons processes any personal data or has control over or authorises the processing of any personal data but does not include a data processor.
Data processor	
Article 4(8): 'processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.	Section 4(18): 'data processor' in relation to personal data, means any person, other than an employee of the data user, who processes the personal data solely on behalf of the data user, and does not process the personal data for any of his own purposes.
Data subject	
Article 4(1): 'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more fPDPAors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.	Section 4(27): 'data subject' means an individual who is the subject of the personal data
Public bodies	
Article 4(7): 'controller' means the natural or legal person, public authority, agency or other body.	Section 3(1): The PDPA shall not apply to the Federal Government and State Governments.

GDPR	PDPA
Nationality of data subject	
Recital 14: The protection afforded by this Regulation should apply to natural persons, whatever their nationality or place of residence, in relation to the processing of their personal data.	The PDPA does not explicitly refer to the nationality of data subjects.
Place of residence	
See Recital 14, above.	The PDPA does not explicitly refer to the data subjects' place of residence.
Deceased individuals	
Recital 27: This Regulation does not apply to the personal data of deceased persons. Member States may provide for rules regarding the processing of personal data of deceased persons.	The PDPA does not explicitly refer to the personal data of deceased persons.

1.2. Territorial scope

Fairly Inconsistent

Both the GDPR and the PDPA have extraterritorial application, applying to data controllers that are not established within their respective jurisdictions, in certain circumstances. Notably, however, the PDPA does not explicitly regulate goods and services or monitoring from abroad, whereas the GDPR explicitly outlines such activity as within its scope.

GDPR	PDPA
Establishment in jurisdiction	
Article 3: This Regulation applies to the processing of personal data in the context of the PDPAivities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not. Recital 22: Establishment implies the effective and real exercise of PDPAivity through stable arrangements.	Section 2(2): [...] The PDPA applies to a person in respect of personal data if: • the person is established in Malaysia and the personal data is processed, whether or not in the context of that establishment, by that person or any other person employed or engaged by that establishment; or • the person is not established in Malaysia but uses equipment in Malaysia for processing the personal data otherwise than for the purposes of transit through Malaysia Section 2(4): [...] The following is to be treated as established in Malaysia: • an individual whose physical presence in Malaysia shall not be less than 180 days in one calendar year; • a body incorporated under the Companies Act 1965; • a partnership or other unincorporated association formed under any written laws in Malaysia; and • any person who does not fall within the above but maintains in Malaysia ° an office, branch, or agency through which he carries on any activity; or ° a regular practice
Extraterritorial	
See Article 3, above.	See Section 2 above.
Goods & servicies from abroad	
Recital 23: In order to ensure that natural persons are not deprived of the protection to which they are entitled under this Regulation, the processing of personal data of data subjects who are in the Union by a controller or a processor not established in the Union should be subject to this Regulation where the processing PDPAivities are related to offering goods or services to such data subjects irrespective of whether connected to a payment.	The PDPA does not refer to the provision of goods and services from abroad.

GDPR	PDPA
Monitoring from abroad	
Recital 24: The processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union should also be subject to this Regulation when it is related to the monitoring of the behaviour of such data subjects in so far as their behaviour takes place within the Union.	The PDPA does not refer to monitoring from abroad.

1.3. Material scope

Fairly consistent

The PDPA and the GDPR adopt similar definitions of general and sensitive personal data, as well as of data processing. In addition, both legislations provide general exceptions for the processing of personal data for purely personal or household activities and enhanced protection for the processing of sensitive and special categories of personal data. However, the PDPA does not directly address anonymous nor pseudonymised data.

GDPR	PDPA
Personal data/ personal information	
Article 4(1): 'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more fPDPAors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.	Section 4(4): 'personal data' means any information in respect of commercial transactions, which: • is being processed wholly or partly by means of equipment operating automatically in response to instructions given for that purpose; • is recorded with the intention that it should wholly or partly be processed by means of such equipment; or • is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system that relates directly or indirectly to a data subject, who is identified or identifiable from that information or from that and other information in the possession of a data user, including any sensitive personal data and expression of opinion about the data subject; but does not include any information that is processed for the purpose of a credit reporting business carried on by a credit reporting agency under the Credit Reporting Agencies Act 2010 ('the Credit Reporting Agencies Act').
Data processing	
Article 4(2): 'processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, 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.	Section 4(19): 'processing', in relation to personal data, means collecting, recording, holding or storing the personal data, or carrying out any operation or set of operations on the personal data, including: • the organisation, adaptation, or alteration of personal data; • the retrieval, consultation, or use of personal data; • the disclosure of personal data by transmission, transfer, dissemination, or otherwise making available; or • the alignment, combination, correction, erasure, or destruction of personal data.

GDPR	PDPA

Special categories of data

Article 9(1): Processing of 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 shall be prohibited.

Section 4(5): 'sensitive personal data' means any personal data consisting of information as to the physical or mental health or condition of a data subject, his political opinions, his religious beliefs or other beliefs of a similar nature, the commission or alleged commission by him of any offence or any other personal data as the Minister may determine by order published in the Federal Government Gazette ('the Gazette').

Anonymised data

Recital 26: The principles of data protection should not apply to anonymous information, namely information which 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 explicitly refer to anonymised data.

Pseudonymised data

Article 4(5): 'pseudonymisation' means the processing of personal data in such a manner that the personal data 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 explicitly refer to pseudonymised data.

Automated processing

Article 2(1): This Regulation applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.

Section 4(5): 'personal data' means any information in respect of commercial transactions, which is being processed wholly or partly by means of equipment operating automatically in response to instructions given for that purpose [...]

GDPR	PDPA

General exemptions

Article 2(2): This Regulation does not apply to the processing of personal data:

(a) in the course of an PDPAivity which falls outside the scope of Union law;

(b) by the Member States when carrying out PDPAivities which fall within the scope of Chapter 2 of Title V of the Treaty on European Union; or

(c) by a natural person in the course of a purely personal or household PDPAivity.

Section 3: The PDPA shall not apply to:

- the Federal Government and State Governments; and
- any personal data processed outside Malaysia unless that personal data is intended to be further processed in Malaysia.

Section 45(1): There shall be an exemption from the provisions of the PDPA for personal data processed by an individual only for the purposes of that individual's personal, family, or household affairs, including recreational purposes.

Further exemptions are provided by Section 45(2) of the PDPA.

2. Key definitions

2.1. Personal data

Fairly consistent

The PDPA largely contains similar definitions to those provided in the GDPR, including personal data which is considered as sensitive or special categories. However, the PDPA does not define 'online identifiers'.

GDPR	PDPA

Personal data/ personal information

Article 4(1): 'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more fPDPAors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Section 4(4): 'personal data' means any information in respect of commercial transactions, which:

- is being processed wholly or partly by means of equipment operating automatically in response to instructions given for that purpose;
- is recorded with the intention that it should wholly or partly be processed by means of such equipment; or
- is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system

that relates directly or indirectly to a data subject, who is identified or identifiable from that information or from that and other information in the possession of a data user, including any sensitive personal data and expression of opinion about the data subject; but does not include any information that is processed for the purpose of a credit reporting business carried on by a credit reporting agency under the Credit Reporting Agencies Act.

Special categories of data

Article 9(1): Processing of 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 shall be prohibited.

Section 4(5): 'sensitive personal data' means any personal data consisting of information as to the physical or mental health or condition of a data subject, his political opinions, his religious beliefs or other beliefs of a similar nature, the commission or alleged commission by him of any offence or any other personal data as the Minister may determine by order published in the Gazette

GDPR	PDPA

Online identifiers

Recital 30: Natural persons may be associated with online identifiers provided by their devices, applications, tools and protocols, such as internet protocol addresses, cookie identifiers or other identifiers such as radio frequency identification tags. This may leave traces which, in particular when combined with unique identifiers and other information received by the servers, may be used to create profiles of the natural persons and identify them.

The PDPA does not explicitly refer to online identifiers.

Third Party

Article 4(9): 'recipient' means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. 2However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing.

Section 4(25): 'third party', in relation to personal data, means any person other than:

- a data subject;
- a relevant person in relation to a data subject;
- a data user;
- a data processor; or
- a person authorised in writing by the data user to process the personal data under the direct control of the data user.

2.2. Pseudonymisation

Unlike the GDPR, the PDPA does not directly define or refer to anonymisation or pseudonymisation of personal data.

GDPR	PDPA
Anonymisation	
Recital 26: 'anonymous information' is information which 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 explicitly refer to anonymous information.
Pseudonymisation	
Article 4(5): 'pseudonymisation' means the processing of personal data in such a manner that the personal data 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 explicitly refer to pseudonymisation.

2.3. Controllers and processors

The PDPA and the GDPR adopt similar concepts of 'controller' and 'processor.' However, the PDPA, unlike the GDPR, does not explicitly define vendor privacy contracts, DPIAs, or DPOs.

GDPR	PDPA
Data controller	
Article 4(7): 'controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.	Section 4(21): 'data user' means a person who either alone or jointly or in common with other persons processes any personal data or has control over or authorises the processing of any personal data but does not include a data processor.
Data processor	
Article 4(8): 'processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.	Section 4(18): 'data processor', in relation to personal data, means any person, other than an employee of the data user, who processes the personal data solely on behalf of the data user, and does not process the personal data for any of his own purposes.
Controller and processor contracts	
Article 28(3): Processing by a processor shall be governed by a contrPDPA or other legal PDPA under Union or Member State law, that is binding on the processor with regard to the controller and that sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller. [Article 28 goes on to stipulate necessary information to be included in such a contrPDPA.]	The PDPA does not refer to controller and processor contracts. However, Section 9(2) of the PDPA states that where processing of personal data is carried out by a data processor on behalf of the data user, the data user shall, for the purpose of protecting the personal data from any loss, misuse, modification, unauthorised or accidental access or disclosure, alteration or destruction, ensure that the data processor: • provides sufficient guarantees in respect of the technical and organisational security measures governing the processing to be carried out; and • takes reasonable steps to ensure compliance with those measures. In addition, Section 6(3) of the Regulations provides that the data user shall ensure that the security standards in the processing activity are complied with by any data processor that carry out the processing on behalf of the data user.

GDPR	PDPA
Data Protection Impact Assessment ('DPIA')	
DPIA is not specifically defined, however Article 35 sets out requirements for DPIAs (see section 5.3. for further information).	The PDPA does not refer to DPIAs.
Data Protection Officer ('DPO')	
DPO is not specifically defined, however Article 37 sets out requirements related to DPOs (see section 5.4. for further information).	The PDPA does not refer to DPOs.

2.4. Children

Fairly inconsistent

Although both the GDPR and the PDPA provide that parental consent is required for the processing of children's data, the PDPA does not explicitly outline additional protections for said processing.

GDPR	PDPA
Children's definition	
The GDPR does not specifically define 'child'. However, Article 8(1) provides: Where point (a) of Article 6(1) applies, in relation to the offer of information society services directly to a child, the processing of the personal data of a child shall be lawful where the child is at least 16 years old. Where the child is below the age of 16 years, such processing shall be lawful only if and to the extent that consent is given or authorised by the holder of parental responsibility over the child. Member States may provide by law for a lower age for those purposes provided that such lower age is not below 13 years.	The PDPA does not specifically define 'child'. However, Section 4(14) of the PDPA states that a 'relevant person,' in relation to a data subject, howsoever described, means in the case of a data subject who is below the age of 18 years, the parent, guardian or person who has parental responsibility for the data subject [...]
Consent for processing children's data	
Article 8(2): The controller shall make reasonable efforts to verify in such cases that consent is given or authorised by the holder of parental responsibility over the child, taking into consideration available technology.	The PDPA does not refer to consent for the processing of children's data. However, Section 3(3) of the Regulations states that a data user shall obtain consent referred to in Section 3(1) from the parent, guardian, or person who has parental responsibility on the data subject, if the data subject is under the age of 18 years.
Privacy notice (children)	
Recital 58: Given that children merit specific protection, any information and communication, where processing is addressed to a child, should be in such a clear and plain language that the child can easily understand.	The PDPA does not provide specific requirements in relation to privacy notices for children.

2.5. Research

Fairly inconsistent

The PDPA and the GDPR both apply to the processing of personal data for scientific/statistical and research purposes. Further to this, both legislations provide certain exemptions to the exercising of data subject rights when conducting processing on this basis. In contrast to the GDPR, however, the PDPA does not define such purposes and is generally less detailed in regard to further processing for compatible purposes.

GDPR	PDPA

Scientific/ historical research definition

Recital 159: Where personal data are processed for scientific research purposes, this Regulation should also apply to that processing. For the purposes of this Regulation, 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.

Recital 160: Where personal data are processed for historical research purposes, this Regulation should also apply to that processing. This should also include historical research and research for genealogical purposes, bearing in mind that this Regulation should not apply to deceased persons.

The PDPA refers to the processing of personal data for statistic and/or research purposes but does not provide definitions thereof.

However, Section 40(4) of the PDPA, dedicated to the processing of sensitive personal data, includes 'medical research' within the definition of 'medical purposes'.

Compatibility with original purpose of collection

Article 5(1)(b): Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation').

The PDPA does not elaborate on whether statistic and/or research purposes must be compatible with the original purpose of collection.

However, Section 45(2)(c) states that personal data processed for preparing statistics or carrying out research shall be exempted from the General Principle, Notice and Choice Principle, Disclosure Principle and Access Principle and other related provisions of the PDPA, provided that such personal data is not processed for any other purpose and that the resulting statistics or the results of the research are not made available in a form which identifies the data subject.

Appropriate safeguards

Article 89(1): Processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, shall be subject to appropriate safeguards, in accordance with this Regulation, for the rights and freedoms of

Please see Section 45(2)(c) above.

GDPR	PDPA

Appropriate safeguards (cont'd)

the data subject. Those safeguards shall ensure that technical and organisational measures are in place in particular in order to ensure respect for the principle of data minimisation. Those measures may include pseudonymisation provided that those purposes can be fulfilled in that manner,

Data subject rights (research)

Under Article 17(3), the right to erasure may not apply in cases of scientific or historical research. Article 21(6), however, provides that data subjects may exercise the right to object to data processing for scientific or historical research purposes. In addition, Article 89 provides that Member States may derogate from the GDPR in regard to data subject rights and data processing for research purposes.

Please see Section 45(2)(c) above.

3. Legal basis

Fairly consistent

The PDPA and the GDPR provide very similar lawful grounds for the processing of personal data, and enhanced protection for the processing of special categories or sensitive data. In addition, both legislations provide exemptions to processing for journalistic, literary, or artistic purposes, as well as conditions for obtaining consent from data subjects.

GDPR	PDPA

Legal grounds

Article 6(1): Processing shall be lawful only if and to the extent that at least one of the following applies:

(a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;

(b) processing is necessary for the performance of a contrPDPA to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contrPDPA;

(c) processing is necessary for compliance with a legal obligation to which the controller is subject;

(d) processing is necessary in order to protect the vital interests of the data subject or of another natural person;

(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; or

(f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

Section 6(1)(a): A data user shall not in the case of personal data other than sensitive personal data, process personal data about a data subject unless the data subject has given their consent to the processing of the personal data.

Section 6(2): Notwithstanding the above, a data user may process personal data about a data subject if the processing is necessary:

- for the performance of a contract to which the data subject is a party;
- for the taking of steps at the request of the data subject with a view to entering into a contract;
- for compliance with any legal obligation to which the data user is the subject, other than an obligation imposed by a contract;
- in order to protect the vital interests of the data subject;
- for the administration of justice; or
- for the exercise of any functions conferred on any person by or under any law.

GDPR	PDPA

Sensitive data (legal basis)

There are specific requirements for processing special categories of data, see Article 9 of the GDPR for further information.

There are specific requirements for processing sensitive data, see Section 40 of the PDPA for further information.

Conditions for consent

Article 7(3): The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw as to give consent.

Article 4: (11) 'consent' of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative PDPAion, signifies agreement to the processing of personal data relating to him or her.

Section 3(1) of the Regulations: A data user shall obtain consent from the data subject in relation to the processing of personal data in any form that such consent can be recorded and maintained properly by the data user.

In addition, Section 3(2) of the Regulations states that if the form in which such content in Section 3(1) is to be given also concerns another matter, the requirement to obtain consent shall be presented distinguishable in its appearance from such other matters.

Finally, Section 3(5) of the Regulations provides that the burden of proof for consent referred to in Section 3(1) shall lie on the data user.

Journalism/artistic purposes

Article 85(1): Member States shall by law reconcile the right to the protection of personal data pursuant to this Regulation with the right to freedom of expression and information, including processing for journalistic purposes and the purposes of academic, artistic or literary expression.

Article 45(2)(f): Processing only for journalistic, literary, or artistic purposes shall be exempted from the General Principle, Notice and Choice Principle, Disclosure Principle, Retention Principle, Data Integrity Principle, and Access Principle and other related provisions of the PDPA, provided that:

- the processing is undertaken with a view to the publication by any person of the journalistic, literary, or artistic material;
- the data user reasonably believes that, taking into account the special importance of public interest in freedom of expression, the publication would be in the public interest; and
- the data user reasonably believes that in all the circumstances, compliance with the provision in respect of which the exemption is claimed is incompatible with the journalistic, literary, or artistic purposes.

4. Controller and processor obligations

4.1. Data transfers

Fairly inconsistent

The PDPA and GDPR both provide for transfers based on adequate protection. However, the PDPA does not outline other mechanisms such as standard contractual clauses ('SCCs') or Binding Corporate Rules ('BCRs') to enable international data transfers; instead, the PDPA provides a number of exceptions, to the general prohibition on international transfers not specified by the Minister, similar to the derogations provided in the GDPR, including consent and performance of the contract.

GDPR	PDPA

Adequate protection

Article 45(1): A transfer of personal data to a third country or an international organisation may take place where the Commission has decided that the third country, a territory or one or more specified sectors within that third country, or the international organisation in question ensures an adequate level of protection. Such a transfer shall not require any specific authorisation.

Section 129(2) of the PDPA provides that, for the purpose of Section 129(1), as outlined below, the Minister may specify any place outside Malaysia if:

- there is in that place in force any law which is substantially similar to the PDPA, or that serves the same purposes as the PDPA;
- or that place ensures an adequate level of protection in relation to the processing of personal data which is at least equivalent to the level of protection afforded by the PDPA.

In addition, Section 129(3)(f) states that a data user may transfer any personal data to a place outside Malaysia if [...] the data user has taken all reasonable precautions and exercised all due diligence to ensure that the personal data will not in that place be processed in any manner which, if that place is Malaysia, would be a contravention of the PDPA.

GDPR	PDPA

Other mechanisms for data transfers

Article 46(1): In the absence of a decision pursuant to Article 45(3), a controller or processor may transfer personal data to a third country or an international organisation only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available.
(2) The appropriate safeguards referred to in paragraph 1 may be provided for, without requiring any specific authorisation from a supervisory authority, by:
(a) a legally binding and enforceable instrument between public authorities or bodies;
(b) binding corporate rules in accordance with Article 47;
(c) standard data protection clauses adopted by the Commission in accordance with the examination procedure referred to in Article 93(2);
(d) standard data protection clauses adopted by a supervisory authority and approved by the Commission pursuant to the examination procedure referred to in Article 93(2);
(e) an approved code of conduct pursuant to Article 40 together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights; or
(f) an approved certification mechanism pursuant to Article 42 together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights.
(3) Subject to the authorisation from the competent supervisory authority, the appropriate safeguards referred to in paragraph 1 may also be provided for, in particular, by:
(a) contrPDPAual clauses between the controller or processor and the controller, processor or the recipient of the personal data in the third country or international organisation; or
(b) provisions to be inserted into administrative arrangements between public authorities or bodies which include enforceable and effective data subject rights.

Section 129(1): A data user shall not transfer any personal data of a data subject to a place outside Malaysia unless to such place as specified by the Minister, upon the recommendation of the PDP by notification published in the Gazette.

Section 129(3): Notwithstanding Section 129(1), a data user may transfer any personal data to a place outside Malaysia if:

- the data subject has given their consent to the transfer;
- the transfer is necessary for the performance of a contract between the data subject and the data user;
- the transfer is necessary for the conclusion or performance of a contract between the data user and a third party which is:
  - entered into at the request of the data subject; or
  - in the interest of the data subject;
- the transfer is for the purpose of any legal proceedings or for the purpose of obtaining legal advice or for establishing, exercising, or defending legal rights;
- the data user has reasonable grounds for believing that in all circumstances of the case:
  - the transfer is for the avoidance or mitigation of adverse action against the data subject;
  - it is not practicable to obtain the consent in writing of the data subject to that transfer; and
  - if it was practicable to obtain such consent, the data subject would have given their consent;
- the data user has taken all reasonable precautions and exercised all due diligence to ensure that the personal data will not be processed in a place, in any manner which, if that place is Malaysia, would be a contravention of the PDPA; and
- the transfer is necessary in order to protect the vital interests of the data subject; or
- the transfer is necessary as being in the public interest in circumstances as determined by the Minister.

GDPR	PDPA
Data localisation	
Not applicable.	Not applicable.

4.2. Data processing records

Fairly consistent

The GDPR and the PDPA both impose an obligation on data controllers to record their processing activities. The GDPR also imposes this obligation on data processors, while the PDPA is silent on the matter. Furthermore, the GDPR describes a list of information that a data controller must record while the PDPA does not.

GDPR	PDPA
Data controller obligation	
Article 30(1): Each controller and, where applicable, the controller's representative, shall maintain a record of processing PDPAivities under its responsibility. That record shall contain all of the following information: (a) the name and contPDPA details of the controller and, where applicable, the joint controller, the controller's representative and the data protection officer; (b) the purposes of the processing; (c) a description of the categories of data subjects and of the categories of personal data; (d) the categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organisations; (e) where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, in the case of transfers referred to in the second subparagraph of Article 49(1), the documentation of suitable safeguards; (f) where possible, the envisaged time limits for erasure of the different categories of data; and (g) where possible, a general description of the technical and organisational security measures referred to in Article 32(1).	Article 44(1): A data user shall keep and maintain a record of any application, notice, request, or any other information relating to personal data that has been or is being processed by him.

GDPR	PDPA

Data processor obligation

GDPR	PDPA
Article 30(2): Each processor and, where applicable, the processor's representative shall maintain a record of all categories of processing PDPAivities carried out on behalf of a controller, containing: (a) the name and contPDPA details of the processor or processors and of each controller on behalf of which the processor is PDPAing, and, where applicable, of the controller's or the processor's representative, and the data protection officer; (b) the categories of processing carried out on behalf of each controller; (c) where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, in the case of transfers referred to in the second subparagraph of Article 49(1), the documentation of suitable safeguards; and (d) where possible, a general description of the technical and organisational security measures referred to in Article 32(1).	The PDPA does not explicitly provide record-keeping requirements applicable to data processors.

Records format

GDPR	PDPA
Article 30(3): The records referred to in paragraphs 1 and 2 shall be in writing, including in electronic form.	Article 44(2): The PDP may determine the manner and form in which the record is to be maintained.

Required to make available

GDPR	PDPA
Article 30(4): The controller or the processor and, where applicable, the controller's or the processor's representative, shall make the record available to the supervisory authority on request.	The PDPA does not provide specific requirements to make data processing record available.

GDPR	PDPA

Exemptions

GDPR	PDPA
Article 30(5): The obligations referred to in paragraphs 1 and 2 shall not apply to an enterprise or an organisation employing fewer than 250 persons unless the processing it carries out is likely to result in a risk to the rights and freedoms of data subjects, the processing is not occasional, or the processing includes special categories of data as referred to in Article 9(1) or personal data relating to criminal convictions and offences referred to in Article 10.	The PDPA does not provide specific exemptions from data processing record requirements.

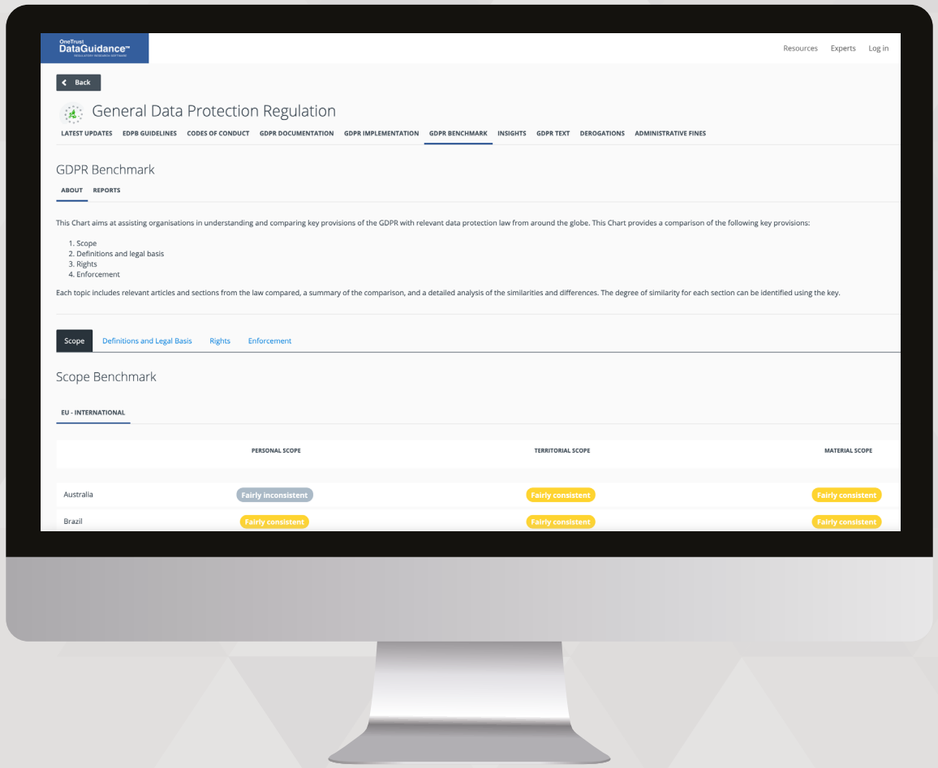
General Data Processing Notification ('DPN')

GDPR	PDPA
Not applicable.	Section 14(1): The Minister may, upon the recommendation of the PDP, by order published in the Gazette, specify a class of data users who shall be required to be registered as data users under this Act. Further to this, Personal Data Protection Order 2013 and the Order 2016 outlines data users that must registered under the PDPA.

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 | China
and 20+ other global laws & frameworks

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

The GDPR Benchmarking tool provides 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

OneTrust
DataGuidance™
REGULATORY RESEARCH SOFTWARE

Start your free trial at
www.dataguidance.com

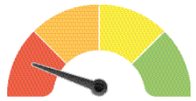
4.3. Data protection impact assessment

Unlike the GDPR, the PDPA does not require or refer to DPIAs.

GDPR	PDPA
When is a DPIA required	
Article 35(1): Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks. [...] (3) A data protection impact assessment referred to in paragraph 1 shall in particular be required in the case of: (a) a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person; (b) processing on a large scale of special categories of data referred to in Article 9(1), or of personal data relating to criminal convictions and offences referred to in Article 10; or (c) a systematic monitoring of a publicly accessible area on a large scale.	The PDPA does not contain requirements to conduct a DPIA.
DPIA content requirements	
Article 35(7): The assessment shall contain at least: (a) a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller; (b) an assessment of the necessity and proportionality of the processing operations in relation to the purposes;	The PDPA does not contain requirements to conduct a DPIA.

GDPR	PDPA
DPIA content requirements (cont'd)	
(c) an assessment of the risks to the rights and freedoms of data subjects referred to in paragraph 1; and (d) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned.	
Consultation with authority	
Article 36(1): The controller shall consult the supervisory authority prior to processing where a data protection impact assessment under Article 35 indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk. [Article 36 goes on to detail requirements related to such prior consultation].	The PDPA does not contain requirements to conduct a DPIA.

4.4. Data protection officer appointment



Unlike the GDPR, the PDPA does not require the appointment of a DPO.

GDPR	PDPA

DPO tasks

GDPR	PDPA
Article 39(1): The data protection officer shall have at least the following tasks: (a) to inform and advise the controller or the processor and the employees who carry out processing of their obligations pursuant to this Regulation and to other Union or Member State data protection provisions; (b) to monitor compliance with this Regulation, with other Union or Member State data protection provisions and with the policies of the controller or 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; (c) to provide advice where requested as regards the data protection impact assessment and monitor its performance pursuant to Article 35; (d) to cooperate with the supervisory authority; and (e) to PDPA as the contPDPA point for 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 PDPA does not mandate the appointment a DPO.

When is a DPO required

GDPR	PDPA
Article 37(1): The controller and the processor shall designate a data protection officer in any case where: (a) the processing is carried out by a public authority or body, except for courts PDPAing in their judicial capacity;	The PDPA does not mandate the appointment a DPO.

GDPR	PDPA

When is a DPO required (cont'd)

GDPR	PDPA
(b) the core PDPAivities of the controller or the 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 (c) the core PDPAivities of the controller or the processor consist of processing on a large scale of special categories of data pursuant to Article 9 and personal data relating to criminal convictions and offences referred to in Article 10.	

Group appointments

GDPR	PDPA
Article 37(2): A group of undertakings may appoint a single data protection officer provided that a data protection officer is easily accessible from each establishment.	The PDPA does not mandate the appointment a DPO.

Notification of DPO

GDPR	PDPA
Article 37(7): The controller or the processor shall publish the contPDPA details of the data protection officer and communicate them to the supervisory authority.	The PDPA does not mandate the appointment a DPO.

Qualifications

GDPR	PDPA
Article 37(5): The data protection officer shall be designated on the basis of professional qualities and, in particular, expert knowledge of data protection law and prPDPAices and the ability to fulfil the tasks referred to in Article 39.	The PDPA does not mandate the appointment a DPO.

4.5. Data security and data breaches

Both the GDPR and the PDPA provide a detailed list of security measures that should be undertaken to avoid data breaches. Unlike the GDPR, the PDPA does not require data breaches to be notified to authorities or data subjects.

GDPR	PDPA

Security measures defined

Article 32(1): Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:

(a) the pseudonymisation and encryption of personal data;

(b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

(c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;

(d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

Section 9(1): A data user shall, when processing personal data, take practical steps to protect the personal data from any loss, misuse, modification, unauthorised or accidental access or disclosure, alteration, or destruction by having regard:

- to the nature of the personal data and the harm that would result from such loss, misuse, modification, unauthorised or accidental access or disclosure, alteration, or destruction;
- to the place or location where the personal data is stored;
- to any security measures incorporated into any equipment in which the personal data is stored;
- to the measures taken for ensuring the reliability, integrity, and competence of personnel having access to the personal data; and
- to the measures taken for ensuring the secure transfer of the personal data.

Section 6(1) of the Regulations further provides that the data user shall develop and implement a security policy for the purposes of Section 9 of the PDPA.

Data breach notification to authority

Article 33(1): In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.

The PDPA does not explicitly require data breach notification to the PDP.

GDPR	PDPA

Timeframe for breach notification

See Article 33(1) above.

Not applicable.

Notifying data subjects of data breach

Article 34(1): When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay.

The PDPA does not explicitly require data breach notification to data subjects.

Data processor notification of data breach

Article 33(2): The processor shall notify the controller without undue delay after becoming aware of a personal data breach.

The PDPA does not explicitly require data processors to report data breaches.

Exceptions

Article 34(3): The communication to the data subject referred to in paragraph 1 shall not be required if any of the following conditions are met:
(a) the controller has implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption;
(b) the controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects referred to in paragraph 1 is no longer likely to materialise;
(c) it would involve disproportionate effort. In such a case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner.

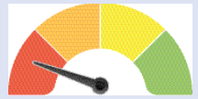
Not applicable.

4.6. Accountability

The PDPA does not contain an express principle of accountability as is the case in the GDPR. However, the PDPA contains provisions such as record keeping and places certain liabilities on data controllers.

GDPR	PDPA
Principle of accountability	
Article 5(2): The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability'). [Paragraph 1 details principles of: lawfulness, fairness and transparency, purpose limitation, data minimisation, accuracy, storage limitation, integrity and confidentiality.]	The PDPA does not contain a specific provision for the principle of accountability. However, certain provisions may be considered to ensure the same, including requirements for data users' registration and record keeping.
Liability of data controllers and data processors	
Article 82(2): Any controller involved in processing shall be liable for the damage caused by processing which infringes this Regulation. A processor shall be liable for the damage caused by processing only where it has not complied with obligations of this Regulation specifically directed to processors or where it has PDPAed outside or contrary to lawful instructions of the controller.	Article 5(2): Subject to Sections 45 and 46, a data user who contravenes the personal data protection principles commits an offence and shall, on conviction, be liable to a fine not exceeding 3,000 (approx. €630) or to imprisonment for a term not exceeding two years or to both

5. Rights



5.1. Right to erasure

Unlike the GDPR, the PDPA does not explicitly refer to a right to erasure.

GDPR	PDPA
Grounds for erasure	
Article 17(1): The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies: (a) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed; (b) the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or point (a) of Article 9(2), and where there is no other legal ground for the processing; (c) the data subject objects to the processing pursuant to Article 21(1) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2); (d) the personal data have been unlawfully processed; (e) the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject; (f) the personal data have been collected in relation to the offer of information society services referred to in Article 8(1).	The PDPA does not explicitly provide for a right to erasure.

GDPR	PDPA

Inform data subject of right

Article 12(1): The controller shall take appropriate measures to provide any information referred to in Articles 13 and 14 and any communication under Articles 15 to 22 and 34 relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child. The information shall be provided in writing, or by other means, including, where appropriate, by electronic means. When requested by the data subject, the information may be provided orally, provided that the identity of the data subject is proven by other means.

The PDPA does not explicitly provide for a right to erasure.

Fees

Article 12(5): Information provided under Articles 13 and 14 and any communication and any PDPAions taken under Articles 15 to 22 and 34 shall be provided free of charge. Where requests from a data subject are manifestly unfounded or excessive, in particular because of their repetitive charPDPAer, the controller may either:

(a) charge a reasonable fee taking into account the administrative costs of providing the information or communication or taking the PDPAion requested; or

(b) refuse to PDPA on the request. The controller shall bear the burden of demonstrating the manifestly unfounded or excessive charPDPAer of the request.

The PDPA does not explicitly provide for a right to erasure.

Response timeframe

Article 12(3): The controller shall provide information on PDPAion taken on a request under Articles 15 to 22 to the data subject without undue delay and in any event within one month of receipt of the request. That period may be extended by two further months where necessary, taking into account the complexity and number of the requests. The controller shall inform the data subject of any such extension within one month of receipt of the request, together with the reasons for the delay. Where the data subject makes the request by electronic form means, the information shall be provided by electronic means where possible, unless otherwise requested by the data subject.

The PDPA does not explicitly provide for a right to erasure.

GDPR	PDPA

Format of response

Article 12(1): The information shall be provided in writing, or by other means, including, where appropriate, by electronic means. When requested by the data subject, the information may be provided orally, provided that the identity of the data subject is proven by other means.

The PDPA does not explicitly provide for a right to erasure.

Publicly available data

Article 17(2): Where the controller has made the personal data public and is obliged pursuant to paragraph 1 to erase the personal data, the controller, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform controllers which are 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.

The PDPA does not explicitly provide for a right to erasure.

Exceptions

Article 17(3): Paragraphs 1 and 2 shall not apply to the extent that processing is necessary:

(a) for exercising the right of freedom of expression and information;

(b) for compliance with a legal obligation which requires processing by Union or Member State law to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

(c) for reasons of public interest in the area of public health in accordance with points (h) and (i) of Article 9(2) as well as Article 9(3);

(d) for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) in so far as the right referred to in paragraph 1 is likely to render impossible or seriously impair the achievement of the objectives of that processing; or

The PDPA does not explicitly provide for a right to erasure.

GDPR	PDPA

Exceptions (cont'd)

(e) for the establishment, exercise or defence of legal claims.

Article 12(5): Information provided under Articles 13 and 14 and any communication and any PDPAions taken under Articles 15 to 22 and 34 shall be provided free of charge. Where requests from a data subject are manifestly unfounded or excessive, in particular because of their repetitive charPDPAer, the controller may either:

(a) charge a reasonable fee taking into account the administrative costs of providing the information or communication or taking the PDPAion requested; or

(b) refuse to PDPA on the request. The controller shall bear the burden of demonstrating the manifestly unfounded or excessive charPDPAer of the request.

The The PDPA does not provide specific exceptions to a right to erasure.

5.2. Right to be informed

Fairly consistent

The PDPA and the GDPR require data controllers to provide information about processing activities to data subjects, irrespective of whether information is collected directly or indirectly from the data subject. Both legislations provide detailed requirements for the disclosure of information that must be given to data subjects and outline requirements for the intelligibility of information. However, the GDPR establishes requirements as to the format in which information is communicated whereas the PDPA does not.

GDPR	PDPA

Informed prior to/ at collection

Article 13(1): Where personal data relating to a data subject are collected from the data subject, the controller shall, at the time when personal data are obtained, provide the data subject with all of the following information:
(a) the identity and the contPDPA details of the controller and, where applicable, of the controller's representative;
(b) the contPDPA details of the data protection officer, where applicable;
(c) the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;
(d) where the processing is based on point (f) of Article 6(1), the legitimate interests pursued by the controller or by a third party;
(e) the recipients or categories of recipients of the personal data, if any;
(f) where applicable, the fPDPA that the controller intends to transfer personal data to a third country or international organisation and the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in Article 46 or 47, or the second subparagraph of Article 49(1), reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available.
(2) In addition to the information referred to in paragraph 1, the controller shall, at the time when personal data are obtained, provide the data subject with the following further information necessary to ensure fair and transparent processing:
(a) the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;
(b) the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability;
(c) where the processing is based on point (a) of Article 6(1) or point (a) of Article 9(2), the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;

Section 7(2): The notice shall be given as soon as practicable by the data user:

- when the data subject is first asked by the data user to provide their personal data;
- when the data user first collects the personal data of the data subject; or
- in any other case, before the data user:
  - uses the personal data of the data subject for a purpose other than the purpose for which the personal data was collected; or
  - discloses the personal data to a third party.

GDPR	PDPA

Informed prior to/ at collection (cont'd)

(d) the right to lodge a complaint with a supervisory authority; (e) whether the provision of personal data is a statutory or contrPDPAual requirement, or a requirement necessary to enter into a contrPDPA, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data; (f) the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

What information is to be provided

See Article 13(1) and (2) above.

Section 7(1): A data user shall by written notice inform a data subject of:

- that personal data of the data subject that is being processed by or on behalf of the data user, and shall provide a description of the personal data to that data subject;
- the purposes for which the personal data is being or is to be collected and further processed;
- of any information available to the data user as to the source of that personal data;
- of the data subject's right to request access to and to request correction of the personal data and how to contact the data user with any inquiries or complaints in respect of the personal data;
- of the class of third parties to whom the data user discloses or may disclose the personal data;
- of the choices and means the data user offers the data subject for limiting the processing of personal data, including personal data relating to other persons who may be identified from that personal data;
- whether it is obligatory or voluntary for the data subject to supply the personal data; and
- where it is obligatory for the data subject to supply the personal data, the consequences for the data subject if they fail to supply the personal data.

GDPR	PDPA

When data is from third party

In addition to the information required under Article 13, Article 14(2) replaces the requirement that data subjects are provided with information on the legitimate interests pursued by the controller or by a third party, with an obligation to inform data subjects of the categories of personal data. Furthermore, paragraph (e) of Article 13(2) is replaced with a requirement to inform data subjects of the source from which the personal data originate, and if applicable, whether it came from publicly accessible sources.

The PDPA does not differentiate between information obtain for the data subject and third parties.

However, the PDP's guidance Know Your Data Privacy Rights states that if an organisation or individual has obtained personal data from others who are not directly the data subject, they must tell the data subject that they are holding the data and notifies the user of the origins.

Intelligibility requirements

Article 12(1): The controller shall take appropriate measures to provide any information referred to in Articles 13 and 14 and any communication under Articles 15 to 22 and 34 relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child. The information shall be provided in writing, or by other means, including, where appropriate, by electronic means. When requested by the data subject, the information may be provided orally, provided that the identity of the data subject is proven by other means.

Section 7(3): A notice shall be in the national and English languages, and the individual shall be provided with a clear and readily accessible means to exercise their choice, where necessary, in the national and English languages.

Format

See Article 12(1) above.

The PDPA does not explicitly address the format of the notice, except for the language requirements outlined above.

Exceptions

The requirements of Article 13 do not apply where the data subject already has the information.
The requirements of Article 14 do not apply where:
(a) the data subject already has the information;
(b) the provision of such information proves impossible or would involve a disproportionate effort, in particular for processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to the conditions and safeguards referred to in Article 89(1)

Section 45(2): Subject to Section 46,

- personal data processed for:
  - the prevention or detection of crime or for the purpose of investigations;
  - the apprehension or prosecution of offenders; or
  - the assessment or collection of any tax or duty or any other imposition of a similar nature, shall be exempted from the General Principle, Notice and Choice Principle, Disclosure Principle and Access Principle and other related provisions of the PDPA;

GDPR	PDPA

Exceptions

or in so far as the obligation referred to in paragraph 1 of this Article is likely to render impossible or seriously impair the achievement of the objectives of that processing. In such cases the controller shall take appropriate measures to protect the data subject's rights and freedoms and legitimate interests, including making the information publicly available;

(c) obtaining or disclosure is expressly laid down by Union or Member State law to which the controller is subject and which provides appropriate measures to protect the data subject's legitimate interests; or

(d) where the personal data must remain confidential subject to an obligation of professional secrecy regulated by Union or Member State law, including a statutory obligation of secrecy.

- processed in relation to information of the physical or mental health of a data subject shall be exempted from the Access Principle and other related provisions of the PDPA of which the application of the provisions to the data subject would be likely to cause serious harm to the physical or mental health of the data subject or any other individual;
- processed for preparing statistics or carrying out research shall be exempted from the General Principle, Notice and Choice Principle, Disclosure Principle and Access Principle and other related provisions of this Act, provided that such personal data is not processed for any other purpose and that the resulting statistics or the results of the research are not made available in a form which identifies the data subject;
- that is necessary for the purpose of or in connection with any order or judgement of a court shall be exempted from the General Principle, Notice and Choice Principle, Disclosure Principle and Access Principle and other related provisions of the PDPA;
- processed for the purpose of discharging regulatory functions shall be exempted from the General Principle, Notice and Choice Principle, Disclosure Principle and Access Principle and other related provisions of this Act if the application of those provisions to the personal data would be likely to prejudice the proper discharge of those functions; or
- processed only for journalistic, literary, or artistic purposes shall be exempted from the General Principle, Notice and Choice Principle, Disclosure Principle, Retention Principle, Data Integrity Principle and Access Principle and other related provisions of the PDPA, provided that:
  - the processing is undertaken with a view to the publication by any person of the journalistic, literary or artistic material;
  - the data user reasonably believes that, taking into account the special importance of public interest in freedom of expression, the publication would be in the public interest; and
  - the data user reasonably believes that in all the circumstances, compliance with the provision in respect of which the exemption is claimed is incompatible with the journalistic, literary, or artistic purposes.

Fairly consistent

5.3. Right to object

The PDPA does not provide a general right to object, instead the legislation provides data subjects with the right to prevent processing likely to cause damage or distress and processing for direct marketing purposes. Both the PDPA and GDPR however, provide a right to withdraw consent and require that data subjects be provided with information about their ability to exercise their rights.

GDPR	PDPA

Grounds for right to object/ opt out

Article 21(1): The data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her which is based on point (e) or (f) of Article 6(1), including profiling based on those provisions. The controller shall no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims.

The PDPA does not provide a general right to object.

However, Section 42(1) provides that, subject to section 42(2), a data subject may, at any time by notice in writing to a data user, referred to as the 'data subject notice', require the data user at the end of such period as is reasonable in the circumstances, to:

- cease the processing of or processing for a specified purpose or in a specified manner; or
- not begin the processing of or processing for a specified purpose or in a specified manner any personal data in respect of which he is the data subject if, based on reasons to be stated by him:
  - the processing of that personal data or the processing of personal data for that purpose or in that manner is causing or is likely to cause substantial damage or substantial distress to him or to another person; and
  - the damage or distress is or would be unwarranted.

Withdraw consent

Article 7(3): The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw as to give consent.

Section 38 (1): A data subject may by notice in writing withdraw their consent to the processing of personal data in respect of which they are the data subject.

Section 38 (2): The data user shall, upon receiving the notice under Section 38(1), cease the processing of the personal data.

Restrict processing

Article 18(1): The data subject shall have the right to obtain from the controller restriction of processing where one of the following applies:

See Section 42(1) above.

GDPR	PDPA

Restrict processing (cont'd)

(a) the accuracy of the personal data is contested by the data subject, for a period enabling the controller to verify the accuracy of the personal data;

(b) the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead;

(c) the controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defence of legal claims;

(d) the data subject has objected to processing pursuant to Article 21(1) pending the verification whether the legitimate grounds of the controller override those of the data subject.

Object to direct marketing

Article 21(3): Where the data subject objects to processing for direct marketing purposes, the personal data shall no longer be processed for such purposes.

Section 43(1): A data subject may, at any time by notice in writing to a data user, require the data user at the end of such period as is reasonable in the circumstances to cease or not to begin processing their personal data for purposes of direct marketing.

Inform data subject of right

See Article 12(1) in section 5.1. above. In addition, Article 21(4) provides: At the latest at the time of the first communication with the data subject, the right referred to in paragraphs 1 and 2 shall be explicitly brought to the attention of the data subject and shall be presented clearly and separately from any other information.

See Section 7(1)(d) in section 6.2. above.

Fees

See Article 12(5) in section 5.1. above.

The PDPA does not address the collection of fees for the right to prevent processing likely to cause damage or distress.

GDPR	PDPA

Response timeframe

See Article 12(3) in section 5.1. above.

Section 42(3): The data user shall, within 21 days from the date of receipt of the data subject notice under Section 42(1), give the data subject a written notice:

- stating that they have complied or intend to comply with the data subject notice; or
- stating their reasons for regarding the data subject notice as unjustified, or to any extent unjustified, and the extent, if any, to which they have complied or intend to comply with it.

Format of response

See Article 12(1) in section 5.1. above.

The PDPA does not specify the format of the response. However, Section 42(3) makes reference to a written notice.

Exceptions

See Article 12(5) in section 5.1. above.

Section 42(2): Section 42(1) shall not apply where:

- the data subject has given their consent;
- the processing of personal data is necessary:
  - for the performance of a contract to which the data subject is a party;
  - for the taking of steps at the request of the data subject with a view to entering a contract;
  - for compliance with any legal obligation to which the data user is the subject, other than an obligation imposed by contract; or
  - in order to protect the vital interests of the data subject; or
  - in such other cases as may be prescribed by the Minister by order published in the Gazette.

5.4. Right of access

Fairly consistent

Similar to the GDPR, the PDPA establishes a right of access to personal data being processed by a data controller. Both legislations detail requirements for the charging of fees, verification of data subjects, format of the response, and provide timeframes in which data controllers must respond. However, the GDPR, unlike the PDPA sets out an extensive list of information that must be provided to the data subject whereas the PDPA does not.

GDPR	PDPA

Grounds for right of access

Article 15(1): The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed.

Section 12: A data subject shall be given access to their personal data held by a data user and be able to correct that personal data where the personal data is inaccurate, incomplete, misleading, or not up-to-date, except where compliance with a request to such access or correction is refused under the PDPA.

Section 30(1): An individual is entitled to be informed by a data user whether personal data of which that individual is the data subject is being processed by or on behalf of the data user.

Information to be accessed

Article 15(1): The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information:

(a) the purposes of the processing;
(b) the categories of personal data concerned;
(c) the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations;
(d) where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;
(e) 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;
(f) the right to lodge a complaint with a supervisory authority;
(g) where the personal data are not collected from the data subject, any available information as to their source; and

Section 30(2)(a): A requestor may, upon payment of a prescribed fee, make a data access request in writing to the data user for information of the data subject's personal data that is being processed by or on behalf of the data user [...].

GDPR	PDPA

Information to be accessed (cont'd)

(h) the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

Inform data subject of right

See Article 12(1) in section 5.1.

See Section 7(1)(d) in section 6.2. above.

Fees

See Article 12(5) in section 5.1. above.

See Section 30(2)(a) above.

In addition, the First Schedule of the Fees Regulation outlines the maximum fees payable for a data access request.

Verify data subject request

Recital 64: The controller should use all reasonable measures to verify the identity of a data subject who requests access, in particular in the context of online services and online identifiers. A controller should not retain personal data for the sole purpose of being able to rePDPA to potential requests.

Section 32(1)(a): A data user may refuse to comply with a data access request if the data user is not supplied with such information as they may reasonably require:

- in order to satisfy themselves as to the identity of the requestor; or
- where the requestor claims to be a relevant person, in order to satisfy themselves:
  - as to the identity of the data subject in relation to whom the requestor claims to be the relevant person; and
  - that the requestor is the relevant person in relation to the data subject.

Section 32(2): In determining for the purposes of Section 32(1)(d)(ii) whether it is reasonable in all the circumstances to comply with the data access request without the consent of the other individual, regard shall be had, in particular, to:

- any duty of confidentiality owed to the other individual;
- any steps taken by the data user with a view to seeking the consent of the other individual;
- whether the other individual is capable of giving consent; and
- any express refusal of consent by the other individual.

GDPR	PDPA

Response timeframe

See Article 12(3) in section 5.1. above.

Section 31(1): Subject to Section 31(2) and Section 32, a data user shall comply with a data access request not later than 21 days from the date of receipt of the data access request.
Section 31(2): A data user who is unable to comply with a data access request within the specified period shall before the expiration of that period:

- by notice in writing inform the requestor that he is unable to comply with the data access request within such period and the reasons why he is unable to do so; and
- comply with the data access request to the extent that he is able to do so.

Section 31(3): Notwithstanding Section 31(2), the data user shall comply in whole with the data access request not later than 14 days after the expiration of the period stipulated.

Format of response

See Article 12(1) in section 5.1. above.

Section 30(2)(b): A requestor may, upon payment of a prescribed fee, make a data access request in writing to the data user [...] to have communicated to them a copy of the personal data in an intelligible form.

Exceptions

See Article 12(5) in section 5.1. above.

Section 32(1): A data user may refuse to comply with:

- a data access request under section 30 if the data user is not supplied with such information as he may reasonably require:
- in order to satisfy themselves as to the identity of the requestor; or
- where the requestor claims to be a relevant person, in order to satisfy themselves:
- as to the identity of the data subject in relation to whom the requestor claims to be the relevant person; and
- that the requestor is the relevant person in relation to the data subject;
- the data user is not supplied with such information as he may reasonably require locating the personal data to which the data access request relates;
- the burden or expense of providing access is disproportionate to the risks to the data subject's privacy

GDPR	PDPA

Exceptions (cont'd)

See Article 12(5) in section 5.1. above.

in relation to the personal data in the case in question;

- the data user cannot comply with the data access request without disclosing personal data relating to another individual who can be identified from that information, unless:
- that other individual has consented to the disclosure of the information to the requestor; or
- it is reasonable in all the circumstances to comply with the data access request without the consent of the other individual;
- subject to exceptions any other data user controls the processing of the personal data to which the data access request relates in such a way as to prohibit the first-mentioned data user from complying, whether in whole or in part, with the data access request;
- providing access would constitute a violation of an order of a court;
- providing access would disclose confidential commercial information; or
- such access to personal data is regulated by another law.
- Section 32(3): Section 32 (1)(e) shall not operate so as to excuse the data user from complying with the data access request to any extent that the data user can comply with the data access request without contravening the prohibition concerned.

5.5. Right not to be subject to discrimination

The PDPA and the GDPR do not specifically refer to a right not to be subject to discrimination. In addition, data subjects have a right not to be subject to automated decision-making under both frameworks.

GDPR	PDPA

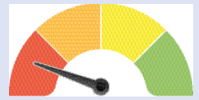
Definition of right

GDPR	PDPA
The GDPR only implies this right and does not provide an explicit definition for it.	The PDPA only implies this right and does not provide an explicit definition for it.

Automated processing

GDPR	PDPA
Article 22(1): The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her. [Article 22 goes on to detail this right, including exceptions]	The PDPA does not explicitly provide data subjects with a right in relation to automated processing. However, the Know Your Rights Guidance provides that data subjects have a right to freedom of automated decision-making.

5.6. Right to data portability



Unlike the GDPR, the PDPA does not explicitly refer to a right to data portability.

GDPR	PDPA

Grounds for portability

GDPR	PDPA
Article 20(1): The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided, where: (a) the processing is based on consent pursuant to point (a) of Article 6(1) or point (a) of Article 9(2) or on a contrPDPA pursuant to point (b) of Article 6(1); and (b) the processing is carried out by automated means.	The PDPA does not explicitly refer to a right to data portability.

Inform data subject of right

GDPR	PDPA
See Article 12(1) in section 5.1.	The PDPA does not explicitly refer to a right to data portability.

Fees

GDPR	PDPA
See Article 12(5) in section 5.1. above.	The PDPA does not explicitly refer to a right to data portability.

Response timeframe

GDPR	PDPA
See Article 12(3) in section 5.1. above.	The PDPA does not explicitly refer to a right to data portability.

Format

GDPR	PDPA
See Article 20(1) above.	The PDPA does not explicitly refer to a right to data portability.

Controller to controller

GDPR	PDPA
Article 20(2): In exercising his or her right to data portability pursuant to paragraph 1, the data subject shall have the right to have the personal data transmitted directly from one controller to another, where technically feasible.	The PDPA does not explicitly refer to a right to data portability.

GDPR	PDPA
Technically feasible	
See Article 20(2) above.	The PDPA does not explicitly refer to a right to data portability.
Exceptions	
See Article 12(5) in section 5.1. above.	The PDPA does not explicitly refer to a right to data portability.

6. Enforcement

6.1. Monetary penalties

The PDPA and the GDPR both provide for the possibility of monetary penalties. However, unlike the GDPR, the PDPA also provides for the possibility of criminal offences, including imprisonment. Moreover, the PDPA does not detail any mitigating factors, and sets out significantly lower fines compared to those provided in the GDPR.

GDPR	PDPA
Provides for monetary penalties	
The GDPR provides for monetary penalties.	The PDPA provides for monetary penalties.
Issued by	
Article 58(2) Each supervisory authority shall have all of the following corrective powers: [...] (i): to impose an administrative fine pursuant to Article 83, in addition to, or instead of measures referred to in this paragraph, depending on the circumstances of each individual case.	Section 49(1): The PDP shall have all such powers to do all things necessary or expedient for or in connection with the performance of their functions under the PDPA. Section 110: The PDP may in writing authorise any officer appointed under Sections 50 and 51 or any public officer to exercise the powers of enforcement under the PDPA.
Fine maximum	
Article 83(5): infringements of the following provisions shall, in accordance with paragraph 2, be subject to administrative fines up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher: (a) the basic principles for processing, including conditions for consent, pursuant to Articles 5, 6, 7 and 9; (b) the data subjects' rights pursuant to Articles 12 to 22; (c) the transfers of personal data to a recipient in a third country or an international organisation pursuant to Articles 44 to 49; (d) any obligations pursuant to Member State law adopted under Chapter IX; (e) non-compliance with an order or a temporary or definitive limitation on processing or the suspension of data flows by the supervisory authority pursuant to Article 58(2) or failure to provide access in violation of Article 58(1).	Section 5(2): Subject to Sections 45 and 46, a data user who contravenes Section 5(1) commits an offence and shall, on conviction, be liable to a fine not exceeding MYR 300,000 (approx. €63,300) or to imprisonment for a term not exceeding two years or to both. Section 16(4): A person who belongs to the class of data users as specified in the order made under Section 14(1) and who processes personal data without a certificate of registration issued in pursuance of Section 16(1)(a) commits an offence and shall, on conviction, be liable to a fine not exceeding MYR 500,000 (approx. €105,480) or to imprisonment for a term not exceeding three years or to both. Section 18(4): A data user whose registration has been revoked under this section and who continues to process personal data thereafter commits an offence and shall, on conviction, be liable to a fine not exceeding MYR 500,000 (approx. €105,480) or to imprisonment for a term not exceeding three years or to both.

GDPR	PDPA

Fine maximum (cont'd)

(6) Non-compliance with an order by the supervisory authority as referred to in Article 58(2) shall, in accordance with paragraph 2 of this Article, be subject to administrative fines up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher.	Section 130(7): A person who commits an offence under Section 130 (unlawful collecting, etc., of personal data) shall, upon conviction, be liable to a fine not exceeding MYR 500,000 (approx. €105,480) or to imprisonment for a term not exceeding three years or to both.

Percentage of turnover

Under Article 83(4), (5), and (6), fines may be issued that equate to 2% or 4% of the total worldwide annual turnover of the preceding financial year.	The PDPA does not provide monetary penalties in the form of percentage of turnover.

Mitigating factors

Article 83(2): When deciding whether to impose an administrative fine and deciding on the amount of the administrative fine in each individual case due regard shall be given to the following: (a) the nature, gravity and duration of the infringement taking into account the nature scope or purpose of the processing concerned as well as the number of data subjects affected and the level of damage suffered by them; (b) the intentional or negligent charPDPAer of the infringement; (c) any PDPAion taken by the controller or processor to mitigate the damage suffered by data subjects; (d) the degree of responsibility of the controller or processor taking into account technical and organisational measures implemented by them pursuant to Articles 25 and 32; (e) any relevant previous infringements by the controller or processor; (f) the degree of cooperation with the supervisory authority, in order to remedy the infringement and mitigate the possible adverse effects of the infringement;	The PDPA does not expressly refer to mitigating factors. However, Section 133(1)(b) of the PDPA states if a body corporate commits an offence under the PDPA, any person who at the time of the commission of the offence was a director, chief executive officer, chief operating officer, manager, secretary or other similar officer of the body corporate or was purporting to act in any such capacity or was in any manner or to any extent responsible for the management of any of the affairs of the body corporate or was assisting in such management [...] if the body corporate is found to have committed the offence, shall be deemed to have committed that offence unless, having regard to the nature of his functions in that capacity and to all circumstances, they prove: • that the offence was committed without their knowledge, consent or connivance; and • that they have taken all reasonable precautions and exercised due diligence to prevent the commission of the offence

GDPR | PDPA

Mitigating factors (cont'd)

(g) the categories of personal data affected by the infringement; (h) the manner in which the infringement became known to the supervisory authority, in particular whether, and if so to what extent, the controller or processor notified the infringement; (i) 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; (j) adherence to approved codes of conduct pursuant to Article 40 or approved certification mechanisms pursuant to Article 42; and (k) any other aggravating or mitigating fPDPAor applicable to the circumstances of the case, such as financial benefits gained, or losses avoided, directly or indirectly, from the infringement.	

Imprisonment

Not applicable.	See Sections16(4), 18(4), and 130(7) above.

DPO liability

Not applicable.	Not applicable

6.2. Supervisory authority

Fairly consistent

The PDPA provides for the establishment of a personal data protection commissioner, currently exercised by the PDP. Similar to the GDPR, the PDP has investigatory, corrective, and advisory powers, and requires the submission of an annual report. In addition, while the PDPA does not outlines specific tasks as provided under the GDPR, the legislation outlines the powers and function of the PDP.

GDPR	PDPA

Provides for data protection authority

Article 51(1): Each Member State shall provide for one or more independent public authorities to be responsible for monitoring the application of this Regulation, in order to protect the fundamental rights and freedoms of natural persons in relation to processing and to facilitate the free flow of personal data within the Union ('supervisory authority').

Section 47(1): The Minister shall appoint any person as the 'Personal Data Protection Commissioner' for the purposes of carrying out the functions and powers assigned to the Commissioner under the PDPA on such terms and conditions as he thinks desirable.

Section 47(3): The Commissioner appointed under Section 47(1) shall be a body corporate having perpetual succession and a common seal.

Investigatory powers

Article 58(1): Each supervisory authority shall have all of the following investigative powers:

(a) to order the controller and the processor, and, where applicable, the controller's or the processor's representative to provide any information it requires for the performance of its tasks;
(b) to carry out investigations in the form of data protection audits;
(c) to carry out a review on certifications issued pursuant to Article 42(7);
(d) to notify the controller or the processor of an alleged infringement of this Regulation;
(e) to obtain, from the controller and the processor, access to all personal data and to all information necessary for the performance of its tasks;
(f) to obtain access to any premises of the controller and the processor, including to any data processing equipment and means, in accordance with Union or Member State procedural law.

Section 105 (1): Where the PDP receives a complaint under Section 104, the PDP shall, subject to Section 106, carry out an investigation in relation to the relevant data user to ascertain whether the act, practice, or request specified in the complaint contravenes the provisions of the PDPA.

Section 105(2): where the PDP has reasonable grounds to believe that an act, practice, or request has been done or engaged in, or is being done or engaged in, by the relevant data user that relates to personal data and such act, practice, or request may be a contravention of the provisions of the PDPA, the PDP may carry out an investigation in relation to the relevant data user to ascertain whether the act, practice, or request contravenes the provisions of the PDPA.

Section 105(3): the provisions of Part IX of the PDPA shall apply in respect of investigations carried out by the PDP under this Part VIII of the PDPA.

GDPR	PDPA

Corrective powers

Article 58(2): Each supervisory authority shall have all of the following corrective powers:
(a) to issue warnings to a controller or processor that intended processing operations are likely to infringe provisions of this Regulation;
(b) to issue reprimands to a controller or a processor where processing operations have infringed provisions of this Regulation;
(c) to order the controller or the processor to comply with the data subject's requests to exercise his or her rights pursuant to this Regulation;
(d) to order the controller or processor to bring processing operations into compliance with the provisions of this Regulation, where appropriate, in a specified manner and within a specified period;
(e) to order the controller to communicate a personal data breach to the data subject;
(f) to impose a temporary or definitive limitation including a ban on processing;
(g) to order the rectification or erasure of personal data or restriction of processing pursuant to Articles 16, 17 and 18 and the notification of such PDPAions to recipients to whom the personal data have been disclosed pursuant to Article 17(2) and Article 19;
(h) to withdraw a certification or to order the certification body to withdraw a certification issued pursuant to Articles 42 and 43, or to order the certification body not to issue certification if the requirements for the certification are not or are no longer met;
(i) to impose an administrative fine pursuant to Article 83, in addition to, or instead of measures referred to in this paragraph, depending on the circumstances of each individual case;
(j) to order the suspension of data flows to a recipient in a third country or to an international organisation.

Section 108(1): Where, following the completion of an investigation about an act, practice, or request specified in the complaint, the PDP is of the opinion that the relevant data user:

- is contravening a provision of the PDPA; or
- has contravened such a provision in circumstances that make it likely that the contravention will continue or be repeated then the PDP may serve on the relevant data user an enforcement notice:
- stating that they are of that opinion;
- specifying the provision of the PDPA on which they have based that opinion and the reasons why they are of that opinion;
- directing the relevant data user to take such steps as are specified in the enforcement notice to remedy the contravention or, as the case may be, the matters occasioning it within such period as is specified in the enforcement notice; and
- directing, where necessary, the relevant data user to cease processing the personal data pending the remedy of the contravention by the relevant data user.

GDPR	PDPA

Authorisation/ advisory powers

Article 58(3): Each supervisory authority shall have all of the following authorisation and advisory powers:
(a) to advise the controller in accordance with the prior consultation procedure referred to in Article 36;
(b) to issue, on its own initiative or on request, opinions to the national parliament, the Member State government or, in accordance with Member State law, to other institutions and bodies as well as to the public on any issue related to the protection of personal data;
(c) to authorise processing referred to in Article 36(5), if the law of the Member State requires such prior authorisation;
(d) to issue an opinion and approve draft codes of conduct pursuant to Article 40(5);
(e) to accredit certification bodies pursuant to Article 43;
(f) to issue certifications and approve criteria of certification in accordance with Article 42(5);
(g) to adopt standard data protection clauses referred to in Article 28(8) and in point (d) of Article 46(2);
(h) to authorise contrPDPAual clauses referred to in point (a) of Article 46(3);
(i) to authorise administrative arrangements referred to in point (b) of Article 46(3);
(j) to approve binding corporate rules pursuant to Article 47.

Section 48(1): The PDP shall have the following functions:

- to advise the Minister on the national policy for personal data protection and all other related matters;
- to implement and enforce the personal data protection laws, including the formulation of operational policies and procedures;
- to promote and encourage associations or bodies representing data users to prepare codes of practice and to disseminate to their members the codes of practice for the purposes of the PDPA;
- to cooperate with bodies corporate or government agencies for the purpose of performing their functions;
- to determine in pursuance of Section 129 whether any place outside Malaysia has in place a system for the protection of personal data that is substantially similar to that as provided for under the PDPA or that serves the same purposes as the PDPA;
- to undertake or cause to be undertaken research into and monitor developments in the processing of personal data, including technology, in order to take account any effects such developments may have on the privacy of individuals in relation to their personal data;
- to monitor and supervise compliance with the provisions of the PDPA, including the issuance of circulars, enforcement notices or any other instruments to any person;
- to promote awareness and dissemination of information to the public about the operation of the PDPA;
- to liaise and cooperate with persons performing similar personal data protection functions in any place outside Malaysia in respect of matters of mutual interest, including matters concerning the privacy of individuals in relation to their personal data;

GDPR	PDPA

Authorisation/ advisory powers (cont'd)

- to represent Malaysia through participation in events that relate to personal data protection as authorised by the Minister, whether within or outside Malaysia; and
- to carry out such activities and do such things as are necessary, advantageous, and proper for the administration of the PDPA, or such other purposes consistent with the PDPA as may be directed by the Minister.

Tasks of authority

Article 57(1): Without prejudice to other tasks set out under this Regulation, each supervisory authority shall on its territory:
(a) monitor and enforce the application of this Regulation;
(b) promote public awareness and understanding of the risks, rules, safeguards and rights in relation to processing. Activities addressed specifically to children shall receive specific attention;
(c) advise, in accordance with Member State law, the national parliament, the government, and other institutions and bodies on legislative and administrative measures relating to the protection of natural persons' rights and freedoms with regard to processing;
(d) promote the awareness of controllers and processors of their obligations under this Regulation;
(e) upon request, provide information to any data subject concerning the exercise of their rights under this Regulation and, if appropriate, cooperate with the supervisory authorities in other Member States to that end;
(f) handle complaints lodged by a data subject, or by a body, organisation or association in accordance with Article 80, and investigate, to the extent appropriate, the subject matter of the complaint and inform the complainant of the progress and the outcome of the investigation within a reasonable period, in particular if further investigation or coordination with another supervisory authority is necessary;
(g) cooperate with, including sharing information and provide mutual assistance to, other supervisory authorities with a view to ensuring the consistency of application and enforcement of this Regulation;
(h) conduct investigations on the application of this Regulation, including on the basis of information received from another supervisory authority or other public authority;

See Section 48(1) above.
Section 49(1): The PDP shall have all such powers to do all things necessary or expedient for or in connection with the performance of their function under the PDPA.
Section 49(2): Without prejudice to the generality of Section 49(1), the powers of the PDP shall include the power without prejudice to the generality of 49(1), the powers of the PDP shall include the power:

- to collect such fees as may be prescribed by the Minister;
- to appoint such agents, experts, consultants, or any other persons as they think fit to assist them in the performance of their function;
- to formulate human resource development and cooperation programmes for the proper and effective performance of their functions;
- to enter into contracts;
- to acquire, purchase, take, hold, and enjoy any movable or immovable property of every description for the performance of their function, and to convey, assign, surrender, yield up, charge, mortgage, demise, transfer, or otherwise dispose of, or deal with such property or any interest therein vested in them;
- to perform such other functions as the Minister may assign from time to time; and
- to do all such things as may be incidental to or consequential upon the performance of their functions.

GDPR	PDPA

Tasks of authority (cont'd)

(i) monitor relevant developments, insofar as they have an impact on the protection of personal data, in particular the development of information and communication technologies and commercial practices;
(j) adopt standard contractual clauses referred to in Article 28(8) and in point (d) of Article 46(2);
(k) establish and maintain a list in relation to the requirement for data protection impact assessment pursuant to Article 35(4);
(l) give advice on the processing operations referred to in Article 36(2);
(m) encourage the drawing up of codes of conduct pursuant to Article 40(1) and provide an opinion and approve such codes of conduct which provide sufficient safeguards, pursuant to Article 40(5);
(n) encourage the establishment of data protection certification mechanisms and of data protection seals and marks pursuant to Article 42(1), and approve the criteria of certification pursuant to Article 42(5);
(o) where applicable, carry out a periodic review of certifications issued in accordance with Article 42(7);
(p) draft and publish the criteria for accreditation of a body for monitoring codes of conduct pursuant to Article 41 and of a certification body pursuant to Article 43;
(q) conduct the accreditation of a body for monitoring codes of conduct pursuant to Article 41 and of a certification body pursuant to Article 43;
(r) authorise contrPDPAual clauses and provisions referred to in Article 46(3);
(s) approve binding corporate rules pursuant to Article 47;
(t) contribute to the PDPAivities of the Board;
(u) keep internal records of infringements of this Regulation and of measures taken in accordance with Article 58(2); and
(v) fulfil any other tasks related to the protection of personal data.

GDPR	PDPA

Annual report

Article 59: Each supervisory authority shall draw up an annual report on its PDPAivities, which may include a list of types of infringement notified and types of measures taken in accordance with Article 58(2). Those reports shall be transmitted to the national parliament, the government and other authorities as designated by Member State law. They shall be made available to the public, to the Commission and to the Board.

Article 60(1): The PDP shall furnish to the Minister and any such public authority as may be directed by the Minister, the returns, reports, accounts, and information with respect to their activity as the Minister may require or direct.

Article 60(2): Without prejudice to the generality of Section 60(1), the PDP shall, as soon as practicable after the end of each financial year, cause to be made and transmitted to the Minister and if so directed by the Minister to any other public authority, a report dealing with the activities of the PDP during the preceding financial year, and the report shall be in such form and shall contain such information relating to the proceedings and policies of the PDP as the Minister may specify.

6.3. Civil remedies for individuals

Unlike the GDPR, the PDPA does not provide data subjects with an independent cause of action.

GDPR	PDPA
Provides for claims/ cause of PDPAion	
Article 79: Without prejudice to any available administrative or non-judicial remedy, including the right to lodge a complaint with a supervisory authority pursuant to Article 77, each data subject shall have the right to an effective judicial remedy where he or she considers that his or her rights under this Regulation have been infringed as a result of the processing of his or her personal data in non-compliance with this Regulation.	The PDPA does not explicitly provide for a private right of action.
Material and non-material damage	
Article 82(1): Any person who has suffered material or non-material damage as a result of an infringement of this Regulation shall have the right to receive compensation from the controller or processor for the damage suffered.	The PDPA does not explicitly provide for a private right of action.
Mandate for representation	
Article 80(1): The data subject shall have the right to mandate a not-for-profit body, organisation or association which has been properly constituted in accordance with the law of a Member State, has statutory objectives which are in the public interest, and is PDPAive in the field of the protection of data subjects' rights and freedoms with regard to the protection of their personal data to lodge the complaint on his or her behalf, to exercise the rights referred to in Articles 77, 78 and 79 on his or her behalf, and to exercise the right to receive compensation referred to in Article 82 on his or her behalf where provided for by Member State law.	The PDPA does not explicitly provide for a private right of action.
Specifies amount for damages	
Not applicable.	The PDPA does not explicitly provide for a private right of action.
Processor liability	
Article 82(2): Any controller involved in processing shall be liable for the damage caused by processing which infringes this Regulation. A processor shall be liable for the damage caused by processing only where it has not complied with obligations of this Regulation specifically directed to processors or where it has PDPAed outside or contrary to lawful instructions of the controller.	The PDPA does not explicitly provide for a private right of action.
Exceptions	
Article 82(3): A controller or processor shall be exempt from liability under paragraph 2 if it proves that it is not in any way responsible for the event giving rise to the damage.	The PDPA does not explicitly provide for a private right of action.