Comparing privacy laws:
GDPR v. PDPA

OneTrust DataGuidance™
REGULATORY RESEARCH SOFTWARE

About the authors

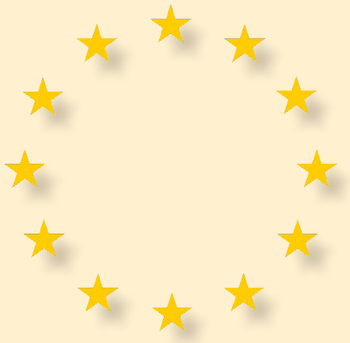
OneTrust DataGuidance™ provides a suite of privacy solutions designed to help organisations monitor regulatory developments, mitigate risk and achieve global compliance.

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 EU and EEA Member States. The Personal Data Protection Act (Act 8/2005) ('PDPA'), which was published in the Government Gazette on 22 August 2005, is the primary legislation governing the processing and protection of personal data in Macau. The PDPA, in accordance with the Chief Executive's Dispatch No. 87/2007 (only available in Chinese and Portuguese here), designated the Office for Personal Data Protection ('GPDP') as the public authority empowered to exercise the duties under the PDPA and responsible for the supervision and coordination thereof. The GPDP has issued a number of guidelines which are accessible here.

On balance, there are broad similarities between the PDPA and the GDPR. Both pieces of legislation employ comparable concepts of personal data, data controllers, and data processors. In addition, both establish similar legal bases for the processing of personal data and for cross-border transfers. However, the PDPA differs from the GDPR in that it focuses primarily on the obligations of controllers, rather than setting out a clear distinction between the responsibilities of controllers and processors. Furthermore, the obligations imposed on controllers and the rights of data subjects are generally less comprehensive than those in the GDPR. For example, the PDPA does not contain record-keeping obligations or requirements as to Data Protection Impact Assessments, nor does it include requirements requiring the notification of data breaches. Overall, the provisions of the PDPA are less onerous than the GDPR, and notably the monetary penalties available for non-compliance are significantly lower.

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 PDPA.

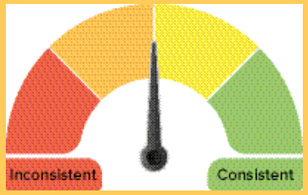
Key for giving the consistency rate

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

Fairly consistent: The GDPR and 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 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 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 acted upon without specific legal advice based on particular circumstances.

1. Scope

Fairly consistent

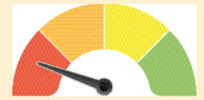
1.1. Personal scope

The PDPA adopts the same key concepts as the GDPR, and both the PDPA and the GDPR apply to individuals as well as private and public bodies. However, the PDPA differs from the GDPR in that it does not specify its applicability based on the nationality or place of residence of the data subject, nor does it clarify its applicability in relation to deceased individuals. Furthermore, unlike the GDPR which contains specific obligations on processors, the PDPA does not regulate processors beyond requiring a contract between controller and processor.

GDPR	PDPA
Similarities	
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.	Article 4(1)(5): 'controller' means the natural or legal person, public entity, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data.
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.	Article 4(1)(6): 'processor' means a natural or legal person, public entity, agency or any other body which processes personal data on behalf of the controller.
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 factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.	Article 4(1)(1): 'personal data' means any information of any type, irrespective of the type of medium involved, including sound and image, relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an indication number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.
Article 4(7): 'controller' means the natural or legal person, public authority, agency or other body.	Article 4(1)(5): 'controller' means the natural or legal person, public entity, agency or any other body.

GDPR	PDPA
Differences	
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.
Regardgin the palce of residence, see Recital 14, above.	The PDPA does not explicitly refer to the place of residence of data subjects.
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



Inconsistent

Unlike the GDPR, the PDPA does not contain a specific provision elaborating on its territorial scope, though the GPDP has confirmed that the PDPA does not apply to the processing of personal data outside of Macau. Nevertheless, the PDPA stipulates that it applies to video surveillance and other forms of sound and image processing to the extent that the controller is based in Macau or makes use of data services provider established in Macau.

GDPR	PDPA
Differences	

1.3. Material scope

While the PDPA and the GDPR employ similar concepts of personal data, data processing, and special or sensitive categories of data, the PDPA does not directly address anonymous and pseudonymous data. Furthermore, the PDPA explicitly provides that it also applies to video surveillance and the processing of personal data for purposes of public safety.

GDPR	PDPA
Similarities	
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 factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.	Article 4(1)(1): 'personal data' means any information of any type, irrespective of the type of medium involved, including sound and image, relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an indication number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.
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.	Article 4(1)(2): 'processing' means any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.
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.	Article 7(1): The processing of personal data revealing philosophical or political beliefs, political society or trade union membership, religion, privacy and racial or ethnic origin, and the processing of data concerning health or sex life, including genetic data, shall be prohibited.

GDPR	PDPA
Differences	
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.
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.
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.	Article 3(1): This Act shall apply to the processing of personal data wholly or partly by automatic means, and to the processing other than by automatic means of personal data which form part of manual filing systems or which are intended to form part of manual filing systems.
Article 2(2): This Regulation does not apply to the processing of personal data: (a) in the course of an activity which falls outside the scope of Union law; (b) by the Member States when carrying out activities 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 activity.	Article 3(2): This Act shall not apply to the processing of personal data carried out by a natural person in the course of a purely personal or household activity, save those with the purposes of systematic communication and dissemination.

2. Key definitions

2.1. Personal data

Fairly consistent

The PDPA largely contains similar definitions as the GDPR, including the types of personal information considered as sensitive or special. However, the PDPA does not define 'online identifiers.'

GDPR	PDPA

Similarities

GDPR	PDPA
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 factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.	Article 4(1)(1): 'personal data' means any information of any type, irrespective of the type of medium involved, including sound and image, relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an indication number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.
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.	Article 7(1): The processing of personal data revealing philosophical or political beliefs, political society or trade union membership, religion, privacy and racial or ethnic origin, and the processing of data concerning health or sex life, including genetic data, shall be prohibited.
Article 4(10): 'third party' means a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data.	Article 4(1)(7): 'third party' means any natural or legal person, public entity, agency or any other body other than the data subject, the controller, the processor and the persons under the direct authority of the controller or the processor, which are qualified to process the data.
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. However, 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.	Article 4(1)(8): 'recipient' means a natural or legal person, public entity, agency or any other body to whom data are disclosed, whether a third party or not; however, authorities which may receive data in the framework of a law or a statutory regulation with [organisational] nature shall not be regarded as recipients.

GDPR	PDPA

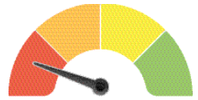
Similarities (cont'd)

GDPR	PDPA
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 action, signifies agreement to the processing of personal data relating to him or her.	Article 4(1)(9): 'the data subject's consent' means any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed.

Differences

GDPR	PDPA
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.

2.2. Pseudonymisation



Inconsistent

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

GDPR	PDPA
Differences	
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.
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

Fairly consistent

Both the PDPA and GDPR define 'controller' and 'processor' in a similar way and refer to the requirement to establish a data processing contract between controller and processor. However, the PDPA differs from the GDPR in that it does not directly address Data Protection Impact Assessments ('DPIA') or the appointment of a data protection officer ('DPO').

GDPR	PDPA
Similarities	
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.	Article 4(1)(5): 'controller' means the natural or legal person, public entity, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data.
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.	Article 4(1)(6): 'processor' means a natural or legal person, public entity, agency or any other body which processes personal data on behalf of the controller.
Article 28(3): Processing by a processor shall be governed by a contract or other legal act 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 contract.]	Article 15(3): The carrying out of processing by way of a processor must be governed by a contract or legal act binding the processor to the controller and stipulating in particular that the processor shall act only on instructions from the controller and that the obligations referred to in [Article 15(1) on security of processing] shall also be incumbent on the processor.
Differences	
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.
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

While the GDPR addresses the processing of children's data and provides additional requirements thereof, the PDPA is silent on this matter. Nevertheless, the GPDP has confirmed that consent from parents or legal guardians is required when processing the data of children below the age of 18.

GDPR	PDPA

Differences

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.

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.

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 address the processing of children's data.

The PDPA does not address consent in relation to the processing of children's data. However, the GPDP has clarified that, pursuant to the Civil Code No. 39/99/M (only available in Chinese here and Portuguese here), children below the age of 18 are incapable of consenting, and therefore consent must be obtained from their parents or legal guardians. See here for example.

The PDPA does not provide specific requirements in relation to the processing of children's data.

2.5. Research

Fairly inconsistent

Both the PDPA and the GDPR apply to the processing of personal data for scientific and historical research purposes, as well as allowing for certain exemptions with regards to data subject rights. In contrast to the GDPR, however, the PDPA does not define such purposes and is generally less detailed in this regard.

GDPR	PDPA

Similarities

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 applies and refers to the processing of personal data for scientific and/or historical purposes in Article 5(2) but does not provide definitions thereof.

Differences

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').

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 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.

The PDPA does not elaborate on whether scientific and/or historical purposes are compatible with the original purpose of collection. However, pursuant to Article 45(3), the GPDP 'may provide that the data held in manual filing systems and kept solely for the purposes of historical research need not be brought into conformity with Articles 7, 8 and 9, provided they are in no case reused for a different purpose.'

[Note: Article 7 governs the processing of personal data, Article 8 regulates data relating to criminal offences, and Article 9 concerns the combination of personal data.]

The PDPA does not contain obligations as to appropriate safeguards that are specific to the processing of personal data for scientific and/or historical purposes.

GDPR	PDPA

Differences (cont'd)

Right of erasure

Under Article 17(3)(d), 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.

Right to be informed

Article 10(5)(3): The obligation to provide information [to data subjects about the processing of personal data] may be waived in the case of scientific and/or historical research when the provision of such information proves impossible or would involve a disproportionate effort or if the recording or disclosure [of such information] is expressly laid down by law or administrative regulations, in which case notification to the [GPDP] is required.

Right of access

Article 11(6): If the data [is] not used for taking measures or decisions regarding any particular individual, the law may restrict the right of access where there is clearly no risk of breaching the fundamental rights, freedoms and guarantees of the data subject, particularly the right to privacy, and when the data [is] used solely for purposes of scientific research or [is] kept in personal form for a period which does not exceed the period necessary for the sole purpose of creating statistics.

3. Legal basis

Fairly consistent

Both the PDPA and the GDPR provide nearly identical legal grounds for the processing of personal data, as well as separate conditions for the processing of special or sensitive data. However, the PDPA is less detailed as to the requirements for obtaining the consent of data subjects.

GDPR	PDPA

Similarities

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 contract 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 contract;

(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.

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

Article 6: Personal data may be processed only if the data subject has unambiguously given his consent or if processing is necessary:

(1) for the performance of a contract or contracts 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 contract or a declaration of his will to negotiate;

(2) for compliance with a legal obligation to which the controller is subject;

(3) in order to protect the vital interests of the data subject if the latter is physically or legally incapable of giving his consent;

(4) for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed;

(5) for pursuing the legitimate interests of the controller or the third party to whom the data are disclosed, except where such interests should be overridden by the interests for fundamental rights, freedoms and guarantees of the data subject.

There are specific requirements for processing sensitive data, see Article 7 of the PDPA for further information.

GDPR	PDPA
Differences	
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.	The PDPA does not outline specific requirements for obtaining consent. Nevertheless, Article 4(1)(9) stipulates that consent means 'any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed.'
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 action, signifies agreement to the processing of personal data relating to him or her.	
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.	The PDPA does not directly address journalistic and/or artistic purposes as a legal basis. Articles 10(6) and 11(3) briefly refer to journalism in the context of data subject rights.

4. Controller and processor obligations

Fairly consistent

4.1. Data transfers

Although both the PDPA and the GDPR prohibit the transfer of personal data to third countries that do not have an adequate level of protection, the PDPA is less comprehensive as to the alternative mechanisms for cross-border data transfers.

GDPR	PDPA
Similarities	
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.	Article 19(1): The transfer of personal data to a destination outside [Macau] may only take place subject to compliance with this Act and provided the legal system in the destination to which they are transferred ensures an adequate level of protection. Article 19(2): The adequacy of the level of protection referred to in the previous number shall be assessed in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations; particular consideration shall be given to the nature of the data, the purpose and duration of the proposed processing operation or operations, the place of origin and place of final destination, the rules of law, both general and sectoral, in force in the destination in question and the professional rules and security measures which are complied with in that destination. Article 19(3): It is for the GPDP to decide whether a legal system ensures an adequate level of protection.

GDPR	PDPA

Differences

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.

Article 46(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) contractual 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

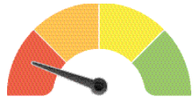
Article 20(2): The GPDP may authorise a transfer or a set of transfers of personal data to a destination in which the legal system does not ensure an adequate level of protection [...], provided the controller adduces adequate safeguards with respect to the protection of the privacy and fundamental rights and freedoms of individuals and with respect to their exercise, particularly by means of appropriate contractual clauses.

GDPR | PDPA

Differences (cont'd)

(b) provisions to be inserted into administrative arrangements between public authorities or bodies which include enforceable and effective data subject rights.

4.2. Data processing records



In contrast to the GDPR, the PDPA does not require controllers or processors to keep records of their processing activities. However, unlike the GDPR, the PDPA establishes a general data processing notification ('DPN') requirement as well as a requirement to obtain prior authorisation from the GPDP for certain types of processing activities.

GDPR	PDPA

Differences

GDPR	PDPA
Article 30(1): Each controller and, where applicable, the controller's representative, shall maintain a record of processing activities under its responsibility. That record shall contain all of the following information: (a) the name and contact 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).	The PDPA does not contain specific record-keeping requirements.
Article 30(2): Each processor and, where applicable, the processor's representative shall maintain a record of all categories of processing activities carried out on behalf of a controller, containing:	The PDPA does not contain specific record-keeping requirements.

GDPR	PDPA

Differences (cont'd)

GDPR	PDPA
(a) the name and contact details of the processor or processors and of each controller on behalf of which the processor is acting, 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).	
Article 30(3): The records referred to in paragraphs 1 and 2 shall be in writing, including in electronic form.	The PDPA does not contain specific record-keeping requirements.
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 contain specific record-keeping requirements.
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 contain specific record-keeping requirements.
Not applicable.	Article 21(1): The controller or his representative, if any, must notify the [GPDP] in written form within eight days after the initiation of carrying out any wholly or partly automatic processing operation or set of such operations intended to serve a single purpose or several related purposes. Article 22(1): The authorisation of the [GPDP] is required for:

GDPR	PDPA

Differences (cont'd)

(1) the processing of personal data referred to in No. 2 of Article 7 [i.e. sensitive personal data];

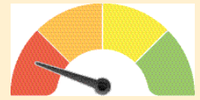
(2) the processing of personal data relating to credit and the solvency of the data subjects;

(3) the combination of personal data provided for in Article 9;

(4) the use of personal data for purposes not giving rise to their collection.

[Note: Applications for opinions, authorisation, and notifications submitted to the GPDP must include the information set out in Article 23 and, where applicable, Article 24. Notifications and authorisations are thereafter publicised in a public register pursuant to Article 25.]

4.3. Data protection impact assessment



Unlike the GDPR, the PDPA does not require or refer to Data Protection Impact Assessments ('DPIA').

GDPR	PDPA

Differences

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.

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;

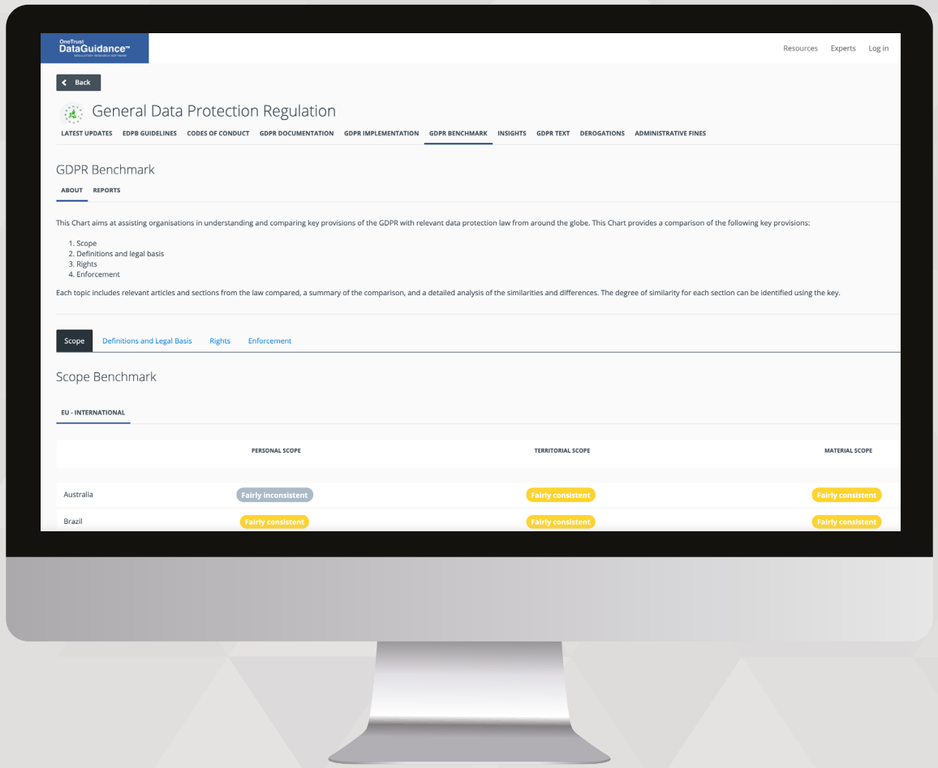
(c) an assessment of the risks to the rights and freedoms of data subjects referred to in paragraph 1; and

The PDPA does not contain requirements to conduct a DPIA.

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

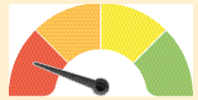
- Employ topic specific guidance to develop your compliance activities
- Monitor news and access written opinion pieces on the most recent developments

OneTrust
DataGuidance™
REGULATORY RESEARCH SOFTWARE

Start your free trial at
www.dataguidance.com

GDPR	PDPA
Differences (cont'd)	
(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.	
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



Inconsistent

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

GDPR	PDPA
Differences	
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 act as the contact 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 explicitly refer to DPOs.
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 acting in their judicial capacity; (b) the core activities 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	The PDPA does not explicitly refer to DPOs. However, the GPDP clarified that although the appointment of an officer in charge of personal data protection is not mandatory, nor required to be reported to the GPDP, it is advisable for organisations to appoint officers in charge of personal data protection in order to better implement the PDPA. See here for example.

GDPR	PDPA
Differences (cont'd)	
(c) the core activities 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.	
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 explicitly refer to DPOs.
Article 37(7): The controller or the processor shall publish the contact details of the data protection officer and communicate them to the supervisory authority.	The PDPA does not explicitly refer to DPOs.
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 practices and the ability to fulfil the tasks referred to in Article 39.	The PDPA does not explicitly refer to DPOs.

4.5. Data security and data breaches

Fairly inconsistent

Whereas the GDPR presents an inexhaustive list of security measures and sets out a comprehensive notification procedure for data breaches, the PDPA provides far less detail and does not require data breaches to be notified to the GPDP or data subjects. Notably, in contrast to the GDPR, the security requirements outlined in the PDPA only directly apply to controllers.

GDPR	PDPA
Similarities	
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.	Article 15(1): The controller must implement appropriate technical and organisational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing. Having regard to the state of the art and the cost of their implementation, such measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected. Article 16(1): [Controllers of sensitive personal data or data concerning criminal offences] shall take appropriate measures to: (1) prevent unauthorised persons from entering the premises used for processing such data (control of entry to the premises); (2) prevent data media from being read, copied, altered or removed by unauthorised persons (control of data media); (3) prevent unauthorised input and unauthorised obtaining of knowledge, alteration or elimination of personal data input (control of input); (4) prevent automatic data processing systems from being used by unauthorised persons by means of data transmission premises (control of use); (5) guarantee that authorised persons may only access data covered by the authorisation (control of access); (6) guarantee the checking of the bodies to whom personal data may be transmitted by means of data transmission premises (control of transmission);

GDPR	PDPA

Similarities (cont'd)

	(7) guarantee that it is possible to check a posteriori, in a period appropriate to the nature of the processing, the establishment in the regulations applicable to each sector of which personal data are input, when and by whom (control of input);
	(8) in transmitting personal data and in transporting the respective media, prevent unauthorised reading, copying, alteration or elimination of data (control of transport).

Differences

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 specifically require the notification of data breaches.
See Article 33(1) above.	The PDPA does not specifically require the notification of data breaches.
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 specifically require the notification of data breaches.
Article 33(2): The processor shall notify the controller without undue delay after becoming aware of a personal data breach.	The PDPA does not specifically require the notification of data breaches.
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;	The PDPA does not specifically require the notification of data breaches.

GDPR | PDPA

Differences (cont'd)

(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.

4.6. Accountability

Fairly inconsistent

The PDPA does not contain an express principle of accountability as is the case in the GDPR. However, the PDPA contains provisions such as the assignment of dedicated personnel which are relevant to the principle and specifies certain liabilities for non-government agencies.

GDPR	PDPA

Differences

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. Guidance from the GPDP, though, confirms that controllers are responsible for complying with the PDPA, including inter alia establishing legitimate processing purposes, respecting legal principles, and ensuring data security. See here for example.

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 acted outside or contrary to lawful instructions of the controller.

While the PDPA does not explicitly define the liabilities of controllers and processors, it does define the offences for which organisations will be liable in the case of non-compliance with the PDPA. See section 6 for further information.

Furthermore, pursuant to Article 14(1), any person who has suffered damage as a result of an unlawful processing operation or of any other act incompatible with legal provisions or regulations in the area of personal data protection is entitled to receive compensation from the controller for the damage suffered.

With regards to liability in relation to processors, the PDPA does not expressly address this matter. However, Article 17 provides that any person acting under the authority of the controller or the processor, including the processor himself, who has access to personal data must not process them except on instructions from the controller, unless he is required to do so by law.

5. Rights

Fairly inconsistent

5.1. Right to erasure

The PDPA differs from the GDPR in that it does not contain a distinct right to erasure, but instead provides for the possibility of erasure as part of a right of access which is generally less comprehensive than the GDPR.

GDPR	PDPA

Similarities

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).

Article 11(1)(4): The data subject has the right to obtain from the controller without constraint at reasonable intervals and without excessive delay or expense the rectification, erasure or blocking of data, the processing of which does not comply with the provisions of [the PDPA], in particular because of the incomplete or inaccurate nature of the data.

GDPR	PDPA

Differences (cont'd)

GDPR	PDPA
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.	Article 10(1): The controller or his representative shall provide a data subject from whom data relating to himself are collected with the following information, except where he already has it: [...] (3) other information such as: [...] (iii) The existence and conditions of the right of access and the right to rectify, provided they are necessary, taking account of the specific circumstances of collection of the data in order to guarantee the data subject that they will be processed fairly.
Article 12(5): Information provided under Articles 13 and 14 and any communication and any actions 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 character, the controller may either: (a) charge a reasonable fee taking into account the administrative costs of providing the information or communication or taking the action requested; or (b) refuse to act on the request. The controller shall bear the burden of demonstrating the manifestly unfounded or excessive character of the request.	Pursuant to Article 11(4), the data subject has the right to obtain erasure from the controller without constraint at reasonable intervals and without excessive delay or expense.
Article 12(3): The controller shall provide information on action 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.	Pursuant to Article 11(4), the data subject has the right to obtain erasure from the controller without constraint at reasonable intervals and without excessive delay or expense.

GDPR | PDPA

Differences (cont'd)

GDPR	PDPA
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 contain any formal requirements as to the format of response.
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.	Article 11(1): The data subject has the right to obtain from the controller without constraint at reasonable intervals and without excessive delay or expense: [...] (5) Notification to third parties to whom the data have been disclosed of any rectification, erasure or blocking carried out in compliance with (4), in which case the third parties are required to rectify, erase or block the data accordingly, unless this proves impossible, or would involve a disproportionate effort.
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 (e) for the establishment, exercise or defence of legal claims.	Article 11(6): If the data are not used for taking measures or decisions regarding any particular individual, the law may restrict the right of access where there is clearly no risk of breaching the fundamental rights, freedoms and guarantees of the data subject, particularly the right to privacy, and when the data are used solely for purposes of scientific research or are kept in personal form for a period which does not exceed the period necessary for the sole purpose of creating statistics. Article 11(1)(5): The data subject has the right to obtain from the controller [...] Notification to third parties to whom the data have been disclosed of any rectification, erasure or blocking [...] in which case the third parties are required to rectify, erase or block the data accordingly, unless this proves impossible, or would involve a disproportionate effort.

GDPR	PDPA

Differences (cont'd)

Article 12(5): Information provided under Articles 13 and 14 and any communication and any actions 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 character, the controller may either:

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

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

5.2. Right to be informed

Fairly consistent

Both the PDPA and GDPR require the controller to provide information about its processing activities to the data subject, whether information is collected directly or indirectly, and both establish similar information requirements and grounds for exemption. Nevertheless, the PDPA is less clear on matters such as intelligibility and format.

GDPR	PDPA

Similarities

Article 13(1) of the GDPR: 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 contact details of the controller and, where applicable, of the controller's representative;

(b) the contact 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 fact 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;

Article 10(1): The controller or his representative shall provide a data subject from whom data relating to himself are collected with the following information, except where he already has it:

(1) the identity of the controller and of his representative, if any;

(2) the purposes of the processing;

(3) other information such as:

(i) The recipients or categories of recipients;

(ii) Whether replies are obligatory or voluntary, as well as the possible consequences of failure to reply;

(iii) The existence and conditions of the right of access and the right to rectify, provided they are necessary, taking account of the specific circumstances of collection of the data in order to guarantee the data subject that they will be processed fairly.

[Note: The GPDP has issued Guidance on the Right to Information in Indirect Collection of Personal Data (August 2010) ('the Guidance') which clarifies that where personal data is collected directly from the data subject, the controller is expected to inform the data subject at the time of collection.]

GDPR	PDPA

Similarities (cont'd)

GDPR	PDPA
(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; (d) the right to lodge a complaint with a supervisory authority; (e) whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, 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.	
See Article 13(1) and (2) above. 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.	See Article 10(1) above. Article 10(3): If the data [is] not collected from the data subject and except where he already has it, the controller or his representative must provide the data subject with the information set down in [Article 10(1)] at the time of undertaking the recording of data or, if a disclosure to third parties is envisaged, no later than the time the data are first disclosed. Article 10(4): If data [is] collected on open networks the data subject shall be informed, except where he is already aware of it, that personal data relating to him may be circulated on the network without security measures and may be at risk of being seen and used by unauthorised third parties.

GDPR	PDPA

Similarities (cont'd)

GDPR	PDPA
	[Note: The GPDP has issued the Guidance which provides further guidance on the timing of informing data subjects, and notably the distinction between the recording and collecting of data. It indicates that in cases where personal data is supplied by an intermediate third party, the obligation to inform the data subject will only materialise when the controller formally records or registers the personal data and involves the same in their processing activities, but not when the data is first supplied.]
The requirements of Article 13 do not apply where the data subject already has the information. Article 14(5): 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) 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.	Article 10(5): The obligation to provide information may be waived by any one of the following: (1) a legal provision; (2) on the grounds of security and criminal prevention or investigation; (3) in particular for processing for statistical purposes or for the purposes of historical or scientific research, when the provision of such information proves impossible or would involve a disproportionate effort or if recording or disclosure is expressly laid down by law or administrative regulations, in which case notification to the public authority is required. Article 10(6): With respect to the basic right of the data subject under [Article 11(3)], the obligation to provide information under this Article shall not apply to the processing of data carried out solely for journalistic purposes or the purpose of artistic or literary expression. [Note: In addition to the above, the obligation to provide information does not apply in cases where the data subject already has the information.]

GDPR	PDPA
Differences	
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 contain any intelligibility requirements in relation to the right to be informed.
See Article 12(1) above.	The PDPA does not contain any formal requirements as to the format. However, the GPDP has issued the Guidance which advises controllers to prepare a 'Personal Data Collection Statement' to be provided to data subjects. Sample statements for reference purposes only have been made available by the GPDP on its website here.

5.3. Right to object

While the PDPA provides for a general right to object and a specific right to object in relation to direct marketing as is the case in the GDPR, the PDPA does not explicitly refer to the withdrawal of consent or a right to restrict processing. Furthermore, unlike the GDPR, the PDPA does not address matters such as fees, timeframes for or format of responses, and exceptions.

GDPR	PDPA
Similarities	
Article 21(1) of the GDPR: 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.	Article 12(1): Save where otherwise provided by law, the data subject has the right to object at any time on compelling legitimate grounds relating to his particular situation to the processing of data relating to him, and where there is a justified objection the processing instigated by the controller may no longer involve those data.
Differences	
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 18(1): The data subject shall have the right to obtain from the controller restriction of processing where one of the following applies: (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;	The PDPA does not explicitly refer to the right to restrict processing.

GDPR	PDPA
Differences (cont'd)	
(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.	
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.	Article 12(2): The data subject also has the right to object, on request and free of charge, to the processing of personal data relating to him which the controller anticipates being processed for the purposes of direct marketing or any other form of commercial research, or to be informed before personal data [is] disclosed for the first time to third parties for the purposes of direct marketing or for use on behalf of third parties, and to be expressly offered the right to object free of charge to such disclosure or uses.
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.	In general, the PDPA does not contain requirements to inform the data subject of the right to object. However, Article 12(2) states that in cases where personal data is disclosed to third parties for the purposes of direct marketing, data subjects must be informed prior to such disclosure and provided with the right to object.
See Article 12(5) in section 5.1. above.	In general, the PDPA does address the matter of fees. However, Article 12(2) states that in case of direct marketing, the data subject has the right to object free of charge.
See Article 12(3) in section 5.1. above.	The PDPA does not contain specific time requirements for responding to requests. However, the data subject can exercise their general right to object at any time.
See Article 12(1) in section 5.1. above.	The PDPA does not contain any formal requirements as to the format of response.
See Article 12(5) in section 5.1. above.	Pursuant to Article 12(1), the right to object applies save as where otherwise provided by law.

5.4. Right of access

Similar to the GDPR, the PDPA establishes a right of access to personal data being processed by the controller. However, while the GDPR sets out extensive obligations and specific conditions as to information and verification requirements, the PDPA does not. In particular, the PDPA does not define explicit exceptions to the right of access, but instead places the authority to review requests relating to certain types of data on the GPDP or the relevant competent authority.

GDPR	PDPA
Similarities	
Article 15(1) of the GDPR: 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.	Article 11(1): The data subject has the right to obtain from the controller without constraint at reasonable intervals and without excessive delay or expense: (1) Confirmation as to whether or not data relating to him [is] being processed and information as to the purposes of the processing, the categories of data concerned and the recipients or categories of recipients to whom the data [is] disclosed; (2) Communication in an intelligible form of the data undergoing processing and of any available information as to their source; (3) Knowledge of the reason involved in any automatic processing of data concerning him.
Differences	
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;	See Article 11(1) above.

GDPR	PDPA
Differences (cont'd)	
(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 (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.	
See Article 12(1) in section 5.1 above.	Article 10(1): The controller or his representative shall provide a data subject from whom data relating to himself are collected with the following information, except where he already has it: [...] (3) other information such as: [...] (iii) The existence and conditions of the right of access and the right to rectify, provided they are necessary, taking account of the specific circumstances of collection of the data in order to guarantee the data subject that they will be processed fairly.
See Article 12(5) in section 5.1. above.	Pursuant to Article 11, the data subject has the right of access without constraint at reasonable intervals and without excessive delay or expense.
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 react to potential requests.	The PDPA does not explicitly refer to identity verification requirements.
See Article 12(3) in section 5.1. above.	Pursuant to Article 11, the data subject has the right to access from the controller without constraint at reasonable intervals and without excessive delay or expense.
See Article 12(1) in section 5.1. above.	Article 11(1)(2) generally requires communication in an intelligible form of the data undergoing processing.

GDPR	PDPA
Differences (cont'd)	
See Article 12(5) in section 5.1. above.	The PDPA provides two scenarios where the right of access may only be exercised by means of the GPDP or the relevant competent authority: in the case of the processing of data relating to security and criminal prevention or investigation (Article 11(2)); or in the case of the processing of data carried out solely for journalistic purposes or the purpose of artistic or literary expression (Articles 11(3) and 10(6)). In this regard, Article 11(4) stipulates that in the cases provided for in [Article 11(2)] and [Article 11(3)], if communication of the data might prejudice security, criminal prevention or investigation and freedom of expression and information or the freedom of the press, the competent authority in that case or the [GPDP] shall only inform the data subject of the measures taken within the limits of maintaining the targeted value of protection described in this [Article]. Furthermore, Article 11(6) provides that if the data [is] not used for taking measures or decisions regarding any particular individual, the law may restrict the right of access where there is clearly no risk of breaching the fundamental rights, freedoms and guarantees of the data subject, particularly the right to privacy, and when the data are used solely for purposes of scientific research or are kept in personal form for a period which does not exceed the period necessary for the sole purpose of creating statistics.

5.5. Right not to be subject to discrimination

Fairly consistent

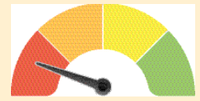
The PDPA and the GDPR do not specifically refer to a right not to be subject to discrimination. However, they both establish rights related to automated decision-making.

GDPR	PDPA

Similarities

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.
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(2) goes on to detail this right, including exceptions]	Article 13(1): Every person shall have the right not to be subject to a decision which produces legal effects concerning him or significantly affects him and which is based solely on automated processing of data intended to evaluate certain personal aspects relating to him, in particular his performance at work, creditworthiness, reliability or conduct. [Article 13(2) goes on to detail this right, including exceptions.]

5.6. Right to data portability



Inconsistent

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

GDPR	PDPA

Differences

GDPR	PDPA
Article 20(1) of the GDPR: 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 contract 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.
See Article 12(1) in section 5.1.	The PDPA does not explicitly refer to a right to data portability.
See Article 12(5) in section 5.1. above.	The PDPA does not explicitly refer to a right to data portability.
See Article 12(3) in section 5.1. above.	The PDPA does not explicitly refer to a right to data portability.
See Article 20(1) above.	The PDPA does not explicitly refer to a right to data portability.
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.
See Article 20(2) above.	The PDPA does not explicitly refer to a right to data portability.
See Article 12(5) in section 5.1. above.	The PDPA does not explicitly refer to a right to data portability.

6. Enforcement

Fairly inconsistent

6.1. Monetary penalties

Both the PDPA and the GDPR provide for the possibility of monetary penalties and other enforcement actions. However, in addition to administrative fines, the PDPA also provides for the possibility of criminal offences, including imprisonment. Nonetheless, the PDPA does not stipulate any mitigating factors and sets out significantly lower fines than the GDPR.

GDPR	PDPA
Similarities	
The GDPR provides for monetary penalties.	The PDPA provides for monetary penalties both under administrative and criminal offences.
Differences	
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.	Article 36(1): The public authority is responsible for the application of the fines provided for in this Act.
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).	Article 32: (1) Bodies which negligently fail to comply with the obligation to notify the public authority of the processing of personal data referred to in [Articles 21(1) and (5)], provide false information or comply with the obligation to notify without observing Article 23 or, having been notified by the public authority, continue to allow access to open data transmission networks to controllers who fail to comply with the provisions of this Act are committing an administrative offence punishable with the following fines: (1) In the case of a natural person, a minimum of MOP 2,000 (approx. €220) and a maximum of MOP 20,000 (approx. €2,200); (2) In the case of a legal person or a body without legal personality, a minimum of MOP 10,000 (approx. €1,100) and a maximum of MOP 100,000 (approx. €11,000). (2) The fine shall be increased to double the maxima in the case of data subject to prior authorisation according to Article 22.

GDPR	PDPA
Differences (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.	Article 33: (1) Bodies which fail to comply with obligations in Articles 5, 10, 11, 12, 13, 16, 17 and [Article 25(3)] are committing an administrative offence punishable with a minimum fine of MOP 4,000 (approx. €440) and a maximum of MOP 40,000 (approx. €4,400). (2) In the case of failure to comply with the obligations in Articles 6, 7, 8, 9, 19 and 20, the administrative offence is punishable with a fine of MOP 8,000 (approx. €880) to MOP 80,000 (approx. €8,800). Article 37 provides that any person who intentionally contravenes obligations relating to personal data protection (as listed in Article 37) is liable for up to one year's imprisonment or a fine of up to 120 days. [See also Articles 38 and 39.]
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.
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 character of the infringement; (c) any action 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;	The PDPA does not expressly refer to mitigating factors.

GDPR	PDPA

Differences (cont'd)

(f) the degree of cooperation with the supervisory authority, in order to remedy the infringement and mitigate the possible adverse effects of the infringement; (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 factor applicable to the circumstances of the case, such as financial benefits gained, or losses avoided, directly or indirectly, from the infringement.	
Not applicable.	Article 37 provides that any person who intentionally contravenes obligations relating to personal data protection (as listed in Article 37) is liable for up to one year's imprisonment or a fine of up to 120 days.

6.2. Supervisory authority

Unlike the GDPR which establishes a data protection authority with extensive powers and duties, the PDPA simply refers to the existence of a 'public authority' to which organisations must notify their processing activities or, where applicable, apply for authorisation. The designation of the GPDP as the public authority referred to in the PDPA is established by the Chief Executive's Dispatch No 87/2007.

GDPR	PDPA

Similarities

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').	The PDPA does not explicitly establish a data protection authority but alludes to its existence and the authority and powers thereof throughout the PDPA. In this regard, the PDPA simply refers to 'the public authority' which was later designated as the GPDP under the Chief Executive's Dispatch No. 87/2007 ('the Executive Dispatch').

Differences

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.	The PDPA does not explicitly refer to investigatory powers.

GDPR	PDPA

Differences (cont'd)

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 actions 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.

The PDPA does not explicitly bestow corrective powers on the GPDP. However, Article 43 provides that the following may be ordered in addition to the fines and penalties provided for in the PDPA:

(1) temporary or permanent prohibition of processing, blocking, erasure or total or partial destruction of data;

(2) publication of the judgement;

(3) public warning or censure of the controller by the [GPDP].

GDPR | PDPA

Differences (cont'd)

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 contractual 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.

Article 22(1): Save where otherwise referred to in [Article 22(2)], the authorisation of the public authority is required for:

(1) the processing of personal data referred to in [Article 7(2)];

(2) the processing of personal data relating to credit and the solvency of the data subjects;

(3) the combination of personal data provided for in Article 9;

(4) the use of personal data for purposes not giving rise to their collection.

[Note: Article 23 also implies the possibility to apply for an opinion from the GPDP.]

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;

The PDPA does not explicitly outline the duties of the GPDP in a comprehensive manner. However, Article 26 states that the [GPDP] shall encourage the drawing up of codes of conduct intended to contribute to the proper implementation of the provisions in [the PDPA], to enhance a great efficacy of self-regulation, and to exercise and protect privacy pertained basic rights, taking account of the specific features of the various sectors.

GDPR	PDPA

Differences (cont'd)

(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;	[Note: The authority of the GPDP is established by the Executive's Dispatch which stipulates in Item No. 2 that the GPDP is authorised to exercise the powers granted by the PDPA and is responsible for monitoring coordinating compliance with the PDPA, implementing the PDPA, as well as developing and implementing a regime for confidentiality.]
(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;	
(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);	

GDPR | PDPA

Differences (cont'd)

(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 contractual clauses and provisions referred to in Article 46(3);	
(s) approve binding corporate rules pursuant to Article 47;	
(t) contribute to the activities 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.	
Article 59: Each supervisory authority shall draw up an annual report on its activities, 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.	The PDPA does not explicitly require the GPDP to draw up an annual report, though Article 25(5) provides that all the opinions and authorisations drawn up or granted under the PDPA [...] must be published by the [GPDP] in its annual report.

6.3. Civil remedies for individuals

Although both the PDPA and the GDPR provide data subjects with an independent cause of action as well as the right to receive compensation for damage suffered as a result of non-compliance, the PDPA does not address matters such as data subject representation and the liability of processors.

GDPR	PDPA

Similarities

GDPR	PDPA
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.	Article 28: Without prejudice to the right to submit a complaint to the public authority, according to the law any individual may have recourse to administrative and legal means to guarantee compliance with legal provisions and statutory regulations in the area of personal data protection.
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.	Article 14(1): Any person who has suffered damage as a result of an unlawful processing operation or of any other act incompatible with legal provisions or regulations in the area of personal data protection is entitled to receive compensation from the controller for the damage suffered. (2) The controller may be exempted from this liability, in whole or in part, if he proves that he is not responsible for the event giving rise to the damage.

Differences

GDPR	PDPA
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 active 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 address the right to mandate representation.
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 acted outside or contrary to lawful instructions of the controller.	The PDPA does not explicitly address the liability of processors in relation to civil remedies. However, Article 14(3) provides that if a processor is involved, Article 492 of the Civil Code (only available in Chinese here and Portuguese here) and its following provisions (i.e. on the apportionment of liability) apply.
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.	Article 14(2): The controller may be exempted from this liability, in whole or in part, if he proves that he is not responsible for the event giving rise to the damage.