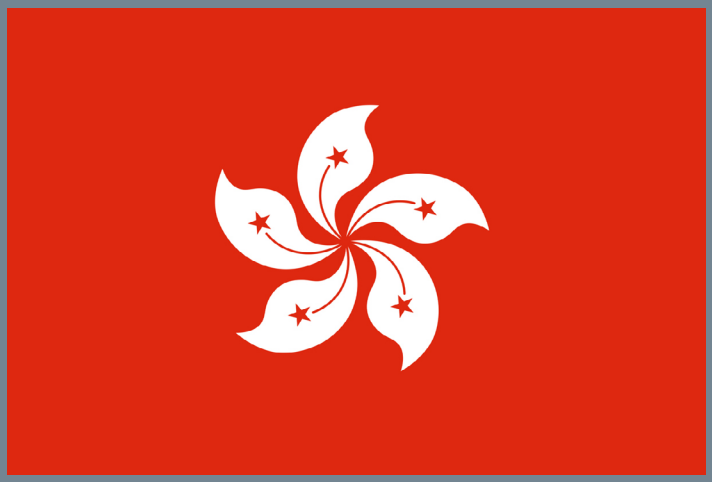


Comparing privacy laws:
GDPR v. PDPO

OneTrust DataGuidance™
REGULATORY RESEARCH SOFTWARE

About the authors

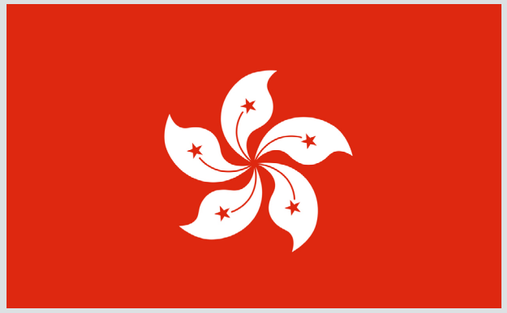
OneTrust DataGuidance™ provides a suite of privacy solutions designed to help organisations monitor regulatory developments, mitigate risk and achieve global compliance.

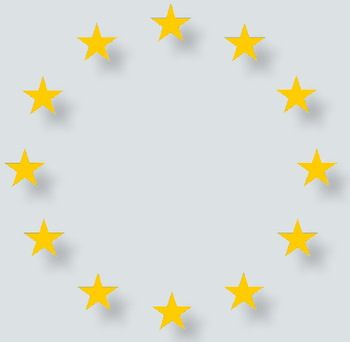
The OneTrust DataGuidance™ platform includes focused guidance around core topics (i.e. GDPR, data transfers, breach notification, among others), Cross-Border Charts which allow you to compare regulations across multiple jurisdictions at a glance, a daily customised news service and expert analysis.

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') came into effect on 25 May 2018, and governs the protection of personal data in EU and EEA Member States. Hong Kong's Personal Data (Privacy) Ordinance (Cap. 486) as amended in 2012 ('PDPO') originally came into effect in 1996 before being significantly amended in 2012. The PDPO established the Office of the Privacy Commissioner for Personal Data ('PCPD'), which has released several pieces of relevant guidance. Please note, the PDPO is referred to as 'the Ordinance' and the PCPD as 'the Commissioner' within the legislation.

Although the PDPO has been in effect for some time, certain provisions, and most notably Section 33 on data transfers, are either not operational or have not been acted upon. There have also been several discussions regarding amending and updating the PDPO as it currently does not address some major topics including mandatory breach notifications. Nonetheless, there are some broad similarities between the PDPO and the GDPR, such as providing for rights of access and correction, the powers afforded to data protection authorities, and in some key definitions. While the PDPO goes into extensive detail in areas such as direct marketing, for the most part it does not provide as comprehensive data protection obligations as the GDPR.

This overview organises provisions from the GDPR and the PDPO 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 PDPO.

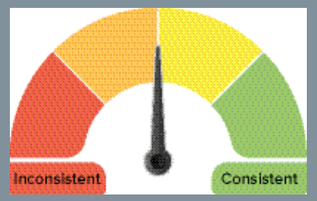
Key for giving the consistency rate

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

Fairly consistent: The GDPR and PDPO 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 PDPO 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 PDPO 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 inconsistent

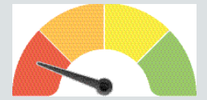
1.1. Personal scope

The concept of a 'data user' within the PDPO is broadly similar to that of a 'data controller' under the GDPR. The applicability of the PDPO on data subjects and public bodies is also largely comparable. However, the PDPO does not regulate data processors beyond requiring a contract between data users and data processors. Furthermore, the PDPO does not specifically clarify its applicability based on the nationality or place of residence of a data subject.

GDPR	PDPO
Similarities	
Article 4(7) of the GDPR: 'controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.	Section 2(1) of the PDPO: 'data user', in relation to personal data, means a person who, either alone or jointly or in common with other persons, controls the collection, holding, processing or use of the data.
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.	Section 2(1): 'data subject', in relation to personal data, means the individual who is the subject of the data.
Article 4(7): 'controller' means the natural or legal person, public authority, agency or other body.	The PCPD has clarified that the PDPO applies to both the private and public sectors.
Differences	
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.	Schedule 1, Principle 2: (4) In subsection (3) – 'data processor' means a person who – (a) processes personal data on behalf of another person; and (b) does not process the data for any of the person's own purposes.
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 PDPO does not explicitly refer to the nationality of data subjects.

Differences (cont'd)	
See Recital 14, above.	The PDPO does not explicitly refer to the place of residence 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 PDPO does not explicitly refer to the personal data of deceased individuals.

1.2. Territorial scope



Inconsistent

The PDPO is unclear on its territorial scope, however the PCPD has clarified that the PDPO does not have extraterritorial scope. In this manner, the PDPO is significantly different from the GDPR, which not only provides for extraterritorial scope but also defines concepts such as being established within the jurisdiction.

GDPR	PDPO
Differences	
Recital 22: Any processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union should be carried out in accordance with this Regulation, regardless of whether the processing itself takes place within the Union. Establishment implies the effective and real exercise of activity through stable arrangements.	The PDPO does not explicitly refer to establishments being based within Hong Kong.
See Recital 22, above.	Although the PDPO does not explicitly refer to this topic, the PCPD has clarified that the PDPO does not have extraterritorial scope.
Recital 23: In order to ensure that natural persons are not deprived of the protection to which they are entitled under this Regulation, the processing of personal data of data subjects who are in the Union by a controller or a processor not established in the Union should be subject to this Regulation where the processing activities are related to offering goods or services to such data subjects irrespective of whether connected to a payment.	The PDPO does not refer to goods & services from abroad.
Recital 24: The processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union should also be subject to this Regulation when it is related to the monitoring of the behaviour of such data subjects in so far as their behaviour takes place within the Union.	The PDPO does not refer to monitoring from abroad.

1.3. Material scope

Fairly inconsistent

While there are similarities between the GDPR and the PDPO in regard to concepts of personal data and data processing, the PDPO does not address notable areas such as sensitive personal data, anonymisation, and pseudonymisation. The PCPD has clarified some of these matters, but the PDPO itself is unclear. However, the PDPO is more detailed and expansive in relation to the exemptions it establishes from its provisions.

GDPR	PDPO
Similarities	
Article 4(1) of the GDPR: '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.	Section 2(1): means any data – (a) relating directly or indirectly to a living individual; (b) from which it is practicable for the identity of the individual to be directly or indirectly ascertained; and (c) in a form in which access to or processing of the data is practicable.
Article 4(2): 'processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.	Section 2(1): 'processing', in relation to personal data, includes amending, augmenting, deleting or rearranging the data, whether by automated means or otherwise.
Differences	
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.	The PDPO does not address special categories of personal data. [Note: Guidance from the PCPD suggests that certain categories of data should be handled differently and refers to the concept of 'sensitive personal data'].
Recital 26: The principles of data protection should not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable.	The PDPO does not refer to anonymised data. [Note: The PCPD has clarified in its Guidance on Personal Data Erasure and Anonymisation (2011) , 'If the personal data held is anonymised to the extent that the data user (or anyone else) will not be able to directly or indirectly identify the individuals concerned, the data is not considered to be personal data under the Ordinance.']
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 PDPO does not 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.	Section 2(1): 'personal data system' means any system, whether or not automated, which is used, whether in whole or in part, by a data user for the collection, holding, processing or use of personal data, and includes any document and equipment forming part of the system. [...] 'processing', in relation to personal data, includes amending, augmenting, deleting or rearranging the data, whether by automated means or otherwise.
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.	Part 8 of the PDPO details several exemptions in both general and specific circumstances. The purposes that either have full or partial exemptions include, among other things, judicial, domestic, employment, security, health, child protection, legal proceedings, statistics and research, news, and due diligence.

2. Key definitions

2.1. Personal data

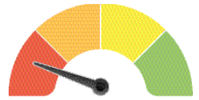
Although the GDPR and the PDPO contain similar definitions for personal data, they differ in regard to special categories of data. Furthermore, an important definition in the PDPO is that of a 'matching procedure', which does not have an equivalent in the GDPR.

GDPR	PDPO
Similarities	
Article 4(1) of the GDPR: '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.	Section 2(1) of the PDPO: means any data – (a) relating directly or indirectly to a living individual; (b) from which it is practicable for the identity of the individual to be directly or indirectly ascertained; and (c) in a form in which access to or processing of the data is practicable.
Differences	
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.	The PDPO does not address special categories of personal data. [Note: Guidance from the PCPD suggests that certain categories of data should be handled differently and refers to the concept of 'sensitive personal data'].
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.	Section 2(1): 'personal identifier' means an identifier – (a) that is assigned to an individual by a data user for the purpose of the operations of the user; and (b) that uniquely identifies that individual in relation to the data user, but does not include an individual's name used to identify that individual.
Not applicable.	Section 2(1): 'matching procedure' means any procedure whereby personal data collected for one or more purposes in respect of 10 or more data subjects is compared (except by manual means) with personal data collected for any other purpose in respect of those data subjects where the comparison –

Differences (cont'd)

PDPO
(a) is (whether in whole or in part) for the purpose of producing or verifying data that; or (b) produces or verifies data in respect of which it is reasonable to believe that it is practicable that the data, may be used (whether immediately or at any subsequent time) for the purpose of taking adverse action against any of those data subjects.

2.2. Pseudonymisation



Unlike the GDPR, the PDPO does not refer to anonymisation or pseudonymisation.

GDPR	PDPO

Differences

GDPR	PDPO
Recital 26 of the GDPR: '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 PDPO does not refer to anonymised data. [Note: The PCPD has released Guidance Note on Personal Data Erasure and Anonymisation.]
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.	Pseudonymisation is not referred to in the PDPO.

2.3. Controllers and processors

There are similarities between the GDPR and the PDPO in relation to definitions of data controllers and data users, data processors, as well as contracts between these parties. Unlike the GDPR, the PDPO does not provide for Data Protection Impact Assessments ('DPIA') or data protection officer ('DPO') appointments.

GDPR	PDPO

Similarities

GDPR	PDPO
Article 4(7) of the GDPR: 'controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.	Section 2(1) of the PDPO: 'data user', in relation to personal data, means a person who, either alone or jointly or in common with other persons, controls the collection, holding, processing or use of the 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.	Schedule 1, Principle 2(4): 'data processor' means a person who – (a) processes personal data on behalf of another person; and (b) does not process the data for any of the person's own purposes.
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.]	Schedule 1, Principle 2(3): Without limiting subsection (2), if a data user engages a data processor, whether within or outside Hong Kong, to process personal data on the data user's behalf, the data user must adopt contractual or other means to prevent any personal data transferred to the data processor from being kept longer than is necessary for processing of the data. Schedule 1, Principle 4(2): Without limiting subsection (1), if a data user engages a data processor, whether within or outside Hong Kong, to process personal data on the data user's behalf, the data user must adopt contractual or other means to prevent unauthorised or accidental access, processing, erasure, loss or use of the data transferred to the data processor for processing.

Differences

GDPR	PDPO
DPIA is not specifically defined, however Article 35 sets out requirements for DPIAs (see section 5.3. for further information).	The PDPO 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 PDPO does not refer to DPOs or an equivalent, except in relation to the contact details of an individual who handles data subject requests being provided to the data subject (see Schedule 1, Principle 1(3)(b)).

2.4. Children

Fairly inconsistent

Both the GDPR and the PDPO refer to children/minors. However, the PDPO does not define an age threshold for minors and is less clear than the GDPR in relation to consent from guardians and privacy notices aimed at minors.

GDPR	PDPO

Similarities

GDPR	PDPO
The GDPR does not specifically define 'child'. However, Article 8(1) provides: Where point (a) of Article 6(1) applies, in relation to the offer of information society services directly to a child, the processing of the personal data of a child shall be lawful where the child is at least 16 years old. Where the child is below the age of 16 years, such processing shall be lawful only if and to the extent that consent is given or authorised by the holder of parental responsibility over the child. Member States may provide by law for a lower age for those purposes provided that such lower age is not below 13 years.	The PDPO makes references to 'minors' but does not define or provide an age threshold for the term.

Differences

GDPR	PDPO
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.	Schedule 1, Principle 3(2): A relevant person in relation to a data subject may, on his or her behalf, give the prescribed consent required for using his/her personal data for a new purpose if – (a) the data subject is – (i) a minor. Section 2(1): 'relevant person', in relation to an individual (howsoever the individual is described), means – (a) where the individual is a minor, a person who has parental responsibility for the minor [...]
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 PDPO does not address this point.

2.5. Research

Fairly inconsistent

While the PDPO provides a general exemption from requirements related to the use of personal data in the context of statistics and research, it provides little detail on this matter. The GDPR sets out particular requirements and exceptions in regard to research.

GDPR	PDPO

Similarities

GDPR	PDPO
Recital 159 of the GDPR: 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.	Although Section 62 the PDPO provides statistics and research with a general exception from data protection principle 3 (regulating the use of personal data), it does not define 'statistics and research'. Section 62: Personal data is exempt from the provisions of data protection principle 3 where – (a) the data is to be used for preparing statistics or carrying out research; (b) the data is not to be used for any other purpose; and (c) the resulting statistics or results of the research are not made available in a form which identifies the data subjects or any of them. [Note: data protection principle 3 regulates the use of personal data, including requirements for obtaining consent for new purposes of processing].
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').	

Differences

GDPR	PDPO
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 PDPO does not explicitly address this point.

GDPR	PDPO

Differences (cont'd)

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

3. Legal basis

Inconsistent

While the GDPR sets out an exhaustive list of legal grounds for the processing of personal data, the PDPO provides a set of data protection principles that must be complied with unless there is an exemption. The laws also differ in regard to special categories of data, exemptions for journalistic and artistic purposes, and conditions for consent.

GDPR	PDPO

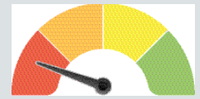
Differences

Article 6(1) of the GDPR: 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.	As opposed to an exhaustive set of legal grounds for processing personal data, the PDPO provides six data protection principles in Schedule 1. These principles regulate: 1. the purpose and manner of collection; 2. accuracy and duration of retention; 3. use of personal data; 4. security of personal data; 5. information to be generally available; and 6. access to personal data. Section 1 defines 'consent' as '**voluntary, specific and informed expression** of will in terms of which permission is given for the processing of personal information.'
There are specific requirements for processing special categories of data, see Article 9 of the GDPR for further information.	The PDPO does not refer to sensitive or special categories of data.
Article 7(3): The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw as to give consent.	Section 2(3): Where under this Ordinance an act may be done with the prescribed consent of a person (and howsoever the person is described), such consent – (a) means the express consent of the person given voluntarily; (b) does not include any consent which has been withdrawn by notice in writing served

GDPR	PDPO
Differences (cont'd)	
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.	on the person to whom the consent has been given (but without prejudice to so much of that act that has been done pursuant to the consent at any time before the notice is so served). [Note: Section 35 provides an alternative definition and set of conditions for consent in the context of direct marketing.]
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.	Section 61: (1) Personal data held by a data user – (a) whose business, or part of whose business, consists of a news activity; and (b) solely for the purpose of that activity (or any directly related activity), is exempt from the provisions of – (i) data protection principle 6 and Section 18(1)(b) and 38(i) unless and until the data is published or broadcast (wherever and by whatever means); (ii) Sections 36 and 38(b). (2) Personal data is exempt from the provisions of data protection principle 3 in any case in which – (a) the use of the data consists of disclosing the data to a data user referred to in subsection (1); and (b) such disclosure is made by a person who has reasonable grounds to believe (and reasonably believes) that the publishing or broadcasting (wherever and by whatever means) of the data (and whether or not it is published or broadcast) is in the public interest. (3) In this Section – 'news activity' means any journalistic activity and includes – (a) the – (i) gathering of news; (ii) preparation or compiling of articles or programmes concerning news; or (iii) observations on news or current affairs, for the purpose of dissemination to the public; or (b) the dissemination to the public of – (i) any article or programme of or concerning news; or (ii) observations on news or current affairs. [Note: The PDPO does not refer to artistic purposes. Section 18 refers to data subject access requests, and Sections 36 and 38 refer to investigations and inspections.]

4. Controller and processor obligations

4.1. Data transfers



Inconsistent

Please note: Section 33 of the PDPO, which regulates data transfers, is not yet operational. In addition, Section 33 only applies to the collection, holding, processing, or use of personal data that takes place in Hong Kong, or is controlled by a data user whose principal place of business is in Hong Kong (including companies incorporated in Hong Kong). Section 35 of the PDPO provides specific requirements for the provision of personal data in the context of direct marketing.

If Section 33 of the PDPO were to come into effect, then it would set a broadly similar basis as the GDPR for the restriction of data transfers. However, Section 33 of the PDPO does not provide for mechanisms such as binding corporate rules ('BCRs') , standard contractual clauses ('SCCs'), or codes of conduct.

GDPR	PDPO
Differences	
Article 45(1): A transfer of personal data to a third country or an international organisation may take place where the Commission has decided that the third country, a territory or one or more specified sectors within that third country, or the international organisation in question ensures an adequate level of protection. Such a transfer shall not require any specific authorisation.	Section 33: (2) A data user shall not transfer personal data to a place outside Hong Kong unless – [...] (b) the user has reasonable grounds for believing that there is in force in that place any law which is substantially similar to, or serves the same purposes as, this Ordinance. [...] (3) Where the Commissioner has reasonable grounds for believing that there is in force in a place outside Hong Kong any law which is substantially similar to, or serves the same purposes as, this Ordinance, he may, by notice in the Gazette, specify that place for the purposes of this Section. (4) Where the Commissioner has reasonable grounds for believing that in a place specified in a notice under subsection (3) there is no longer in force any law which is substantially similar to, or serves the same purposes as, this Ordinance, he shall, either by repealing or amending that notice, cause that place to cease to be specified for the purposes of this Section.
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.	Section 33(2): A data user shall not transfer personal data to a place outside Hong Kong unless – (a) the place is specified for the purposes of this Section in a notice under subsection (3);

GDPR	PDPO

Differences (cont'd)

(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

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

(b) the user has reasonable grounds for believing that there is in force in that place any law which is substantially similar to, or serves the same purposes as, this Ordinance;

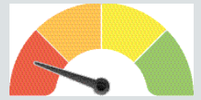
(c) the data subject has consented in writing to the transfer;

(d) the user has reasonable grounds for believing that, in all the circumstances of the case – (i) the transfer is for the avoidance or mitigation of adverse action against the data subject; (ii) it is not practicable to obtain the consent in writing of the data subject to that transfer; and (iii) if it was practicable to obtain such consent, the data subject would give it;

(e) the data is exempt from data protection principle 3 by virtue of an exemption in Part 8; or

(f) the user has taken all reasonable precautions and exercised all due diligence to ensure that the data will not, in that place, be collected, held, processed or used in any manner which, if that place were Hong Kong, would be a contravention of a requirement under this Ordinance.

4.2. Data processing records



Unlike the GDPR, the PDPO does not provide that general data processing records are maintained. However, the PDPO does require that a log book be maintained in relation to data subject access and correction requests.

GDPR	PDPO

Differences

Article 30(1) of the GDPR: 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 PDPO does not contain any general requirements for maintaining data processing records. Section 27 of the PDPO requires that data users maintain a log book in relation to data subject access and correction requests.

Section 27: (2) A data user shall in accordance with subsection (3) enter in the log book – (a) where pursuant to Section 20 the data user refuses to comply with a data access request, particulars of the reasons for the refusal;

(b) where pursuant to Section 21(2) the data user does not comply with Section 21(1), particulars of the prejudice that would be caused to the interest protected by the exemption concerned under Part 8 if the existence or non-existence of the personal data to which the data access request concerned relates was disclosed;

(c) where pursuant to Section 24 the data user refuses to comply with Section 23(1) in relation to a data correction request, particulars of the reasons for the refusal;

(d) any other particulars required by regulations made under Section 70 to be entered in the log book.

(3) The particulars required by subsection (2) to be entered by a data user in the log book shall be so entered – (a) in the case of particulars referred to in paragraph (a) of that subsection, on or before the notice under Section 21(1) is served in respect of the refusal to which those particulars relate;

(b) in the case of particulars referred to in paragraph (b) of that subsection, on or before the notice under Section 21(1) is served in respect of the refusal to which those particulars relate;

(c) in the case of particulars referred to in paragraph (c) of that subsection, on or before the notice under Section 25(1) is served in respect of the refusal to which those particulars relate;

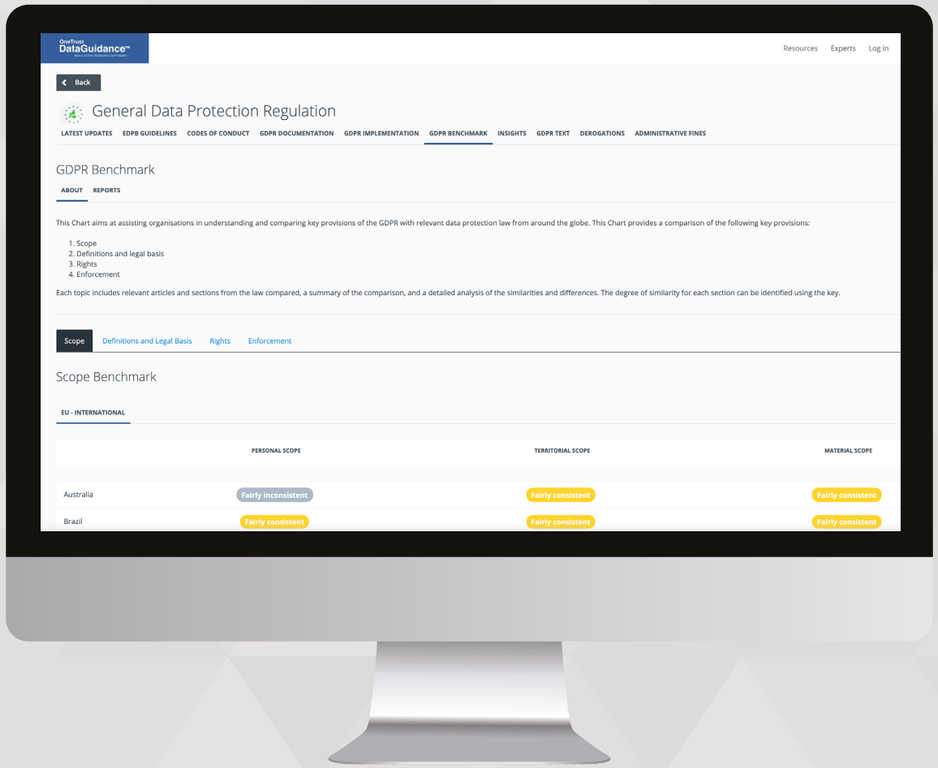
GDPR	PDPO
Differences (cont'd)	
	(d) in the case of particulars referred to in paragraph (d) of that subsection, within the period specified in regulations made under Section 70 in respect of those particulars.
Article 30(2): Each processor and, where applicable, the processor's representative shall maintain a record of all categories of processing activities carried out on behalf of a controller, containing: (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).	The PDPO does not address this topic.
Article 30(3): The records referred to in paragraphs 1 and 2 shall be in writing, including in electronic form.	The PDPO does not contain any general requirements for maintaining data processing records. In relation to the log book required for data subject access and correction requests, Section 27(1) provides: A data user shall keep and maintain a log book – (a) for the purposes of this Part; (b) in the Chinese or English language; and (c) such that any particulars entered in the log book pursuant to this Section are not erased therefrom before the expiration of – (i) subject to subparagraph (ii), four years after the day on which they were so entered; (ii) such longer or shorter period as may be prescribed, either generally or in any particular case, by regulations made under Section 70.

GDPR	PDPO
Differences (cont'd)	
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 PDPO does not contain any general requirements for maintaining data processing records. In relation to the log book required for data subject access and correction requests, Section 27(4) provides: A data user shall – (a) permit the Commissioner to inspect and copy the log book (or any part thereof) at any reasonable time; and (b) without charge, afford the Commissioner such facilities and assistance as the Commissioner may reasonably require for the purposes of such inspection and copying.
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.	There are no specific exemptions from the log book provided for in the PDPO. See Part 8 of the PDPO for general exemptions.
Not applicable.	Part 4, Sections 14-17 of the PDPO provide for a data user return scheme that would require notification of certain information to the PCPD by a selection of data users. However, these provisions have not yet been implemented.

Global Regulatory Research Software

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

Monitor regulatory developments, mitigate risk, and achieve global compliance



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

CCPA | Russia | Thailand | Brazil | Japan | China
and 20+ other global laws & frameworks

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

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

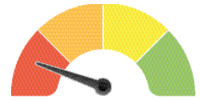
- Scope
- Rights
- Definitions and legal basis
- Enforcement

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

OneTrust
DataGuidance™
REGULATORY RESEARCH SOFTWARE

Start your free trial at
www.dataguidance.com

4.3. Data protection impact assessment



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

GDPR	PDPO

Differences

Article 35(1) of the GDPR: 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 PDPO does not refer to impact assessments.

[Note: the PCPD has recommended Privacy Impact Assessments in certain circumstances. See: Privacy Impact Assessments.]

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 PDPO does not refer to impact assessments.

GDPR	PDPO

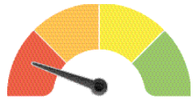
Differences (cont'd)

(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 PDPO does not refer to impact assessments.

4.4. Data protection officer appointment



Unlike the GDPR, the PDPO does not require data protection officer ('DPO') appointments. The PDPO does, however, provide that the contact details of the individual handling access and correction requests be supplied to data subjects. Additionally, the PDPC has published the Privacy Management Programme: A Best Practice Guide (as updated in 2019), recommending the appointment of a DPO.

GDPR	PDPO
Differences	
Article 39(1) of the GDPR: 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 PDPO does not provide requirements for DPO appointments.
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	The PDPO does not provide requirements for DPO appointments.

GDPR	PDPO
Differences (cont'd)	
nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale; or (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 PDPO does not provide requirements for DPO appointments.
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.	Although the PDPO does not provide requirements for DPO appointments, Schedule 1, Principle 1(b) stipulates: [the data subject] is explicitly informed – [...] (ii) on or before first use of the data for the purpose for which it was collected, of – [...] (B) the name or job title, and address, of the individual who is to handle any such request made to the data user.
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 PDPO does not provide requirements for DPO appointments.

4.5. Data security and data breaches

Fairly inconsistent

While the PDPO sets out general security requirements in its fourth data protection principle, these are relatively undefined as compared to the GDPR. Furthermore, the PDPO does not provide for data breach notifications.

GDPR	PDPO

Similarities

GDPR	PDPO
Article 32(1) of the GDPR: 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.	Schedule 1, Principle 4(1): All practicable steps shall be taken to ensure that any personal data (including data in a form in which access to or processing of the data is not practicable) held by a data user is protected against unauthorised or accidental access, processing, erasure, loss or use having particular regard to – (a) the kind of data and the harm that could result if any of those things should occur; (b) the physical location where the data is stored; (c) any security measures incorporated (whether by automated means or otherwise) into any equipment in which the data is stored; (d) any measures taken for ensuring the integrity, prudence and competence of persons having access to the data; and (e) any measures taken for ensuring the secure transmission of the data.

Differences

GDPR	PDPO
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 PDPO does not provide for data breach notifications. [Note: the PCPD has published Guidance on Data breach Handling and the Giving of Breach Notifications.]

GDPR	PDPO

Differences (cont'd)

GDPR	PDPO
See Article 33(1) above.	The PDPO does not provide for data breach notifications.
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 PDPO does not provide for data breach notifications.
Article 33(2): The processor shall notify the controller without undue delay after becoming aware of a personal data breach.	The PDPO does not provide for data breach notifications.
Article 34(3): The communication to the data subject referred to in paragraph 1 shall not be required if any of the following conditions are met: (a) the controller has implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption; (b) the controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects referred to in paragraph 1 is no longer likely to materialise; (c) it would involve disproportionate effort. In such a case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner.	The PDPO does not provide for data breach notifications.

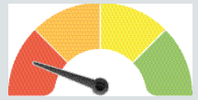
4.6. Accountability

Fairly consistent

Although the PDPO establishes that data user liabilities in greater detail than the GDPR, it is less explicit in setting accountability as a core principle.

GDPR	PDPO
Similarities	
Article 5(2) of the GDPR: 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.]	Accountability is not one of the six data protection principles in the PDPO. However, the PDPO implies accountability requirements throughout its provisions.
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 PDPO sets out data user liabilities throughout its provisions, and particularly in relation to direct marketing and data subject requests. In addition, Section 64A provides more generally that: (1) A data user who, without reasonable excuse, contravenes any requirement under this Ordinance commits an offence and is liable on conviction to a fine at HKD 10,000 (approx. €1,060). (2) Subsection (1) does not apply in relation to – (a) a contravention of a data protection principle; (b) a contravention that constitutes an offence under Section 14(11), 14A(6), (7) or (8), 15(4A) or (7), 18(5), 22(4), 31(4), 32(5), 44(10), 46(11), 50A(1) or (3), 50B(1), 63B(5) or 64(1) or (2); or (c) a contravention of any requirement under Part 6A.

5. Rights



Inconsistent

5.1. Right to erasure

Unlike the GDPR, the PDPO does not provide data subjects with the right to request the erasure or deletion of their personal data. There are only general requirements relating to the erasure of data once it is no longer required for the purpose for which it was collected.

GDPR	PDPO
Differences	
Article 17(1): The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies: (a) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed; (b) the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or point (a) of Article 9(2), and where there is no other legal ground for the processing; (c) the data subject objects to the processing pursuant to Article 21(1) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2); (d) the personal data have been unlawfully processed; (e) the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject; (f) the personal data have been collected in relation to the offer of information society services referred to in Article 8(1).	The PDPO does not provide data subjects with a specific right to request the erasure or deletion of personal data. Section 26 provides: (1) A data user must take all practicable steps to erase personal data held by the data user where the data is no longer required for the purpose (including any directly related purpose) for which the data was used unless – (a) any such erasure is prohibited under any law; or (b) it is in the public interest (including historical interest) for the data not to be erased. (2) For the avoidance of doubt, it is hereby declared that – (a) a data user must take all practicable steps to erase personal data in accordance with subsection (1) notwithstanding that any other data user controls (whether in whole or in part) the processing of the data; (b) the first-mentioned data user shall not be liable in an action for damages at the suit of the second-mentioned data user in respect of any such erasure.

GDPR	PDPO
Differences (cont'd)	
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 PDPO does not provide data subjects with a specific right to request the erasure or deletion of personal data.
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.	The PDPO does not provide data subjects with a specific right to request the erasure or deletion of personal data.
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.	The PDPO does not provide data subjects with a specific right to request the erasure or deletion of personal data.

GDPR	PDPO
Differences (cont'd)	
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 PDPO does not provide data subjects with a specific right to request the erasure or deletion of personal data.
Article 17(2): Where the controller has made the personal data public and is obliged pursuant to paragraph 1 to erase the personal data, the controller, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform controllers which are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data.	The PDPO does not provide data subjects with a specific right to request the erasure or deletion of personal data. [Note: Schedule 1, Principle 2(c) requires that data users inform third parties where personal data is inaccurate.]
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.	The PDPO does not provide data subjects with a specific right to request the erasure or deletion of personal data.

GDPR	PDPO

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

Data protection principle 1 of the PDPO requires information to be provided to data subjects in a similar fashion as the GDPR. However, the PDPO is less detailed on matters such as intelligibility, format, and modifications to information that must be provided to data subject when personal data is obtained from third parties.

GDPR	PDPO

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;

Schedule 1, Principle 1(3) of the PDPO: Where the person from whom personal data is or is to be collected is the data subject, all practicable steps shall be taken to ensure that –

(a) he is explicitly or implicitly informed, on or before collecting the data, of – (i) whether it is obligatory or voluntary for him to supply the data; and (ii) where it is obligatory for him to supply the data, the consequences for him if he fails to supply the data; and

(b) he is explicitly informed – (i) on or before collecting the data, of – (A) the purpose (in general or specific terms) for which the data is to be used; and (B) the classes of persons to whom the data may be transferred; and (ii) on or before first use of the data for the purpose for which it was collected, of – (A) his rights to request access to and to request the correction of the data; and (B) the name or job title, and address, of the individual who is to handle any such request made to the data user,

unless to comply with the provisions of this subsection would be likely to prejudice the purpose for which the data was collected and that purpose is specified in Part 8 of this Ordinance as a purpose in relation to which personal data is exempt from the provisions of data protection principle 6.

[Note: there are specific obligations for information to be provided to data subjects in the context of direct marketing (see Section 35 of the PDPO).]

GDPR	PDPO

Similarities (cont'd)

GDPR	PDPO
(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.	See data protection principle 1 (Schedule 1, Principle 1) above, and Section 35 of the PDPO in the context of direct marketing.
In addition to the information required under Article 13, Article 14(2) replaces the requirement that data subjects are provided with information on the legitimate interests pursued by the controller or by a third party, with an obligation to inform data subjects of the categories of personal data. Furthermore, paragraph (e) of Article 13(2) is replaced with a requirement to inform data subjects of the source from which the personal data originate, and if applicable, whether it came from publicly accessible sources.	The PDPO does not explicitly address this matter except in the context of direct marketing, where it is stipulated in Section 35C(3) that Subsection (1) applies irrespective of whether the personal data is collected from the data subject by the data user.

GDPR	PDPO

Differences

GDPR	PDPO
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 PDPO does not address this matter in general terms. However, in the context of direct marketing, Section 35 of the PDPO specifies that information, such as the kinds and uses of personal data, 'must be presented in a manner that is easily understandable and, if in written form, easily readable.'
See Article 12(1) above.	The PDPO does not explicitly address this matter.
The requirements of Article 13 do not apply where the data subject already has the information.	Section 63C(1): Personal data is exempt from the provisions of data protection principle 1(3) and data protection principle 3 if the application of those provisions to the data would be likely to prejudice any of the following matters –
The requirements of Article 14 do not apply where: (a) the data subject already has the information;	(a) identifying an individual who is reasonably suspected to be, or is, involved in a life-threatening situation;
(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;	(b) informing the individual's immediate family members or relevant persons of the individual's involvement in the life-threatening situation;
(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	(c) the carrying out of emergency rescue operations or provision of emergency relief services.
(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.	

5.3. Right to object

Although the PDPO does not provide for a general right to object, it does include the concept of 'no objection' within its definition of consent in relation to direct marketing. Similarly, within the context of direct marketing, there are provisions for data subjects to request the cessation of processing.

GDPR	PDPO

Similarities

GDPR	PDPO
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.	The PDPO does not provide for a general right to object or opt out. However, in the context of direct marketing, it is stipulated that data users must 'provide the data subject with a channel through which the data subject may, without charge by the data user, communicate the data subject's consent to the intended use.' (Section 35C(2)(c)). Section 35A(1) clarifies, 'consent in relation to a use of personal data in direct marketing or a provision of personal data for use in direct marketing, includes an indication of no objection to the use or provision'.
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.	In the context of direct marketing, the PDPO stipulates that data users must 'provide the data subject with a channel through which the data subject may, without charge by the data user, communicate the data subject's consent to the intended use.' (Section 35C(2)(c)). Section 35A(1) clarifies, 'consent in relation to a use of personal data in direct marketing or a provision of personal data for use in direct marketing, includes an indication of no objection to the use or provision'.

Differences

GDPR	PDPO
Article 7(3): The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw as to give consent.	Section 2(3): Where under this Ordinance an act may be done with the prescribed consent of a person (and howsoever the person is described), such consent – (a) means the express consent of the person given voluntarily; (b) does not include any consent which has been withdrawn by notice in writing served on the person to whom the consent has been given (but without prejudice to so much of that act that has been done pursuant to the consent at any time before the notice is so served).
Article 18(1): The data subject shall have the right to obtain from the controller restriction of processing where one of the following applies:	The PDPO does not provide a general right to restrict processing.

GDPR	PDPO

Differences (cont'd)

GDPR	PDPO
(a) the accuracy of the personal data is contested by the data subject, for a period enabling the controller to verify the accuracy of the personal data; (b) the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead; (c) the controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defence of legal claims; (d) the data subject has objected to processing pursuant to Article 21(1) pending the verification whether the legitimate grounds of the controller override those of the data subject.	Section 35G: (1) A data subject may, at any time, require a data user to cease to use the data subject's personal data in direct marketing. (2) Subsection (1) applies irrespective of whether the data subject – (a) has received from the data user the information required to be provided in relation to the use of personal data under Section 35C(2); or (b) has earlier given consent to the data user or a third person to the use. (3) A data user who receives a requirement from a data subject under subsection (1) must, without charge to the data subject, comply with the requirement. (4) A data user who contravenes subsection (3) commits an offence and is liable on conviction to a fine of HKD 500,000 [approx. €52,900] and to imprisonment for three years. (5) In any proceedings for an offence under subsection (4), it is a defence for the data user charged to prove that the data user took all reasonable precautions and exercised all due diligence to avoid the commission of the offence. (6) This Section does not affect the operation of Section 26 [on erasing personal data after it has been used for specified purpose].
See Article 12(1) in section 6.1. 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.	This is not applicable in general terms under the PDPO. See Section 35C above in regard to direct marketing.
See Article 12(5) in section 5.1. above.	The PDPO does not address this matter in relation to a right to object in general terms. A request to cease processing for direct marketing must be complied with 'without charge to the data subject' (Section 35G(3) of the PDPO).

GDPR	PDPO
Differences (cont'd)	
See Article 12(3) in section 5.1. above.	The PDPO does not address this matter in relation to a right to object.
See Article 12(1) in section 5.1. above.	The PDPO does not address this matter in relation to a right to object.
See Article 12(5) in section 5.1. above.	The PDPO does not address this matter in relation to a right to object in general terms. The provisions related to direct marketing do not apply 'to the offering, or advertising of the availability, of – (a) social services run, subvented or subsidised by the Social Welfare Department; (b) health care services provided by the Hospital Authority or Department of Health; or (c) any other social or health care services which, if not provided, would be likely to cause serious harm to the physical or mental health of –(i) the individual to whom the services are intended to be provided; or (ii) any other individual.

Fairly inconsistent

5.4. Right of access

Both the GDPR and the PDPO provide for the right of access. The PDPO specifies that access is a data protection principle (Schedule 1, Principle 6), and sets out extensive requirements relating to the exercise of this right. While there are general similarities between the GDPR and the PDPO, they differ significantly in their detailing of the right of access.

GDPR	PDPO
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.	Section 18(1) of the PDPO: An individual, or a relevant person on behalf of an individual, may make a request – (a) to be informed by a data user whether the data user holds personal data of which the individual is the data subject; (b) if the data user holds such data, to be supplied by the data user with a copy of such data.
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; (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;	Section 19: (1) Subject to subsection (2) and Sections 20 and 28(5), a data user must comply with a data access request within 40 days after receiving the request by – (a) if the data user holds any personal data which is the subject of the request – (i) informing the requestor in writing that the data user holds the data; and (ii) supplying a copy of the data; or (b) if the data user does not hold any personal data which is the subject of the request, informing the requestor in writing that the data user does not hold the data. [...] (2) A data user who is unable to comply with a data access request within the period specified in subsection (1) shall – (a) before the expiration of that period – (i) by notice in writing inform the requestor that the data user is so unable and of the reasons why the data user is so unable; and (ii) comply with the request to the extent, if any, that the data user is able to comply with the request; and (b) as soon as practicable after the expiration of that period, comply or fully comply, as the case may be, with the request.

GDPR	PDPO
Differences (cont'd)	
(g) where the personal data are not collected from the data subject, any available information as to their source; and	(3) A copy of the personal data to be supplied by a data user in compliance with a data access request shall –
(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.	(a) be supplied by reference to the data at the time when the request is received except that the copy may take account of – (i) any processing of the data –(A) made between that time and the time when the copy is supplied; and (B) that would have been made irrespective of the receipt of the request; and (ii) subject to subsection (5), any correction to the data made between that time and the time when the copy is supplied;
	(b) where any correction referred to paragraph (a) (ii) has been made to the data, be accompanied by a notice stating that the data has been corrected pursuant to that paragraph (or words to the like effect).
See Article 12(1) in section 5.1. above.	Schedule 1, Principle 1(3): Where the person from whom personal data is or is to be collected is the data subject, all practicable steps shall be taken to ensure that – [...] (b) he is explicitly informed – (ii) on or before first use of the data for the purpose for which it was collected, of – (A) his rights to request access to and to request the correction of the data.
See Article 12(5) in section 5.1. above.	Section 28: (1) A data user shall not impose a fee for complying or refusing to comply with a data access request or data correction request unless the imposition of the fee is expressly permitted by this Section.
	(2) Subject to subsections (3) and (4), a data user may impose a fee for complying with a data access request.
	(3) No fee imposed for complying with a data access request shall be excessive.
	(4) Where pursuant to Section 19(3)(c)(iv) or (v) or (4)(ii)(B) (II) a data user may comply with a data access request by supplying a copy of the personal data to which the request relates in one of two or more forms, the data user shall not, and irrespective of the form in which the data user complies with the request, impose a fee for complying with the request which is higher than the lowest fee the data user imposes for complying with the request in any of those forms.

GDPR	PDPO
Differences (cont'd)	
	(5) A data user may refuse to comply with a data access request unless and until any fee imposed by the data user for complying with the request has been paid.
	(6) Where – (a) a data user has complied with a data access request by supplying a copy of the personal data to which the request relates; and (b) the data subject, or a relevant person on behalf of the data subject, requests the data user to supply a further copy of that data,
	then the data user may, and notwithstanding the fee, if any, that the data user imposed for complying with that data access request, impose a fee for supplying that further copy which is not more than the administrative and other costs incurred by the data user in supplying that further copy.
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.	Section 20(1): A data user shall refuse to comply with a data access request - (a) if the data user is not supplied with such information as the data user may reasonably require -
	(i)in order to satisfy the data user as to the identity of the requestor;
	(ii)where the requestor purports to be a relevant person, in order to satisfy the data user - (A) as to the identity of the individual in relation to whom the requestor purports to be such a person; and (B) that the requestor is such a person in relation to that individual.
See Article 12(3) in section 5.1. above.	Section 19: Subject to subsection (2) and Sections 20 and 28(5), a data user must comply with a data access request within 40 days after receiving the request.
See Article 12(1) in section 5.1. above.	Section 19: (3) A copy of the personal data to be supplied by a data user in compliance with a data access request shall – [...] (c) as far as practicable, be –
	(i) intelligible unless the copy is a true copy of a document which – (A) contains the data; and (B) is unintelligible on its face;

GDPR	PDPO
Differences (cont'd)	
	(ii) readily comprehensible with any codes used by the data user adequately explained; and (iii) in – (A) subject to sub-subparagraph (B), the language specified in the request or, if no language is so specified, the language in which the request is made (which may be the Chinese or English language in either case); (B) a language other than the language specified in the request or, if no language is so specified, the language in which the request is made, if, but only if – (I) the language in which the data is held is not the language specified in the request or, if no language is so specified, the language in which the request is made, as the case may be; and (II) subject to Section 20(2)(b), the copy is a true copy of a document which contains the data; (iv) without prejudice to the generality of subparagraph (iii) but subject to subsection (4), be in the form, or one of the forms, if any, specified in the request;
Recital 64: The controller should use all reasonable measures to verify the identity of a data subject who requests access, in particular in the context of online services and online identifiers. A controller should not retain personal data for the sole purpose of being able to react to potential requests.	(v) where subparagraph (iv) is not applicable, in such form as the data user thinks fit. (4) Where – (a) a data access request specifies the form or forms in which a copy of the personal data to be supplied in compliance with the request is or are sought; and (b) the data user concerned is unable to supply the copy in that form or any of those forms, as the case may be, because it is not practicable for the data user to do so, then the data user shall – (i) where there is only one form in which it is practicable for the data user to supply the copy, supply the copy in that form accompanied by a notice in writing informing the requestor that that form is the only form in which it is practicable for the data user to supply the copy;
See Article 12(3) in section 5.1. above. See Article 12(1) in section 5.1. above.	(ii) in any other case – (A) as soon as practicable, by notice in writing inform the requestor – (I) that it is not practicable for the data user to supply the copy in the form or any of the forms, as the case may be, specified in the request; (II) of the forms in which it is practicable for the data user to supply the copy; and (III) that the requestor may, not later than 14 days after the requestor has received the notice, specify in writing one

GDPR	PDPO
Differences (cont'd)	
	of the forms referred to in sub-subparagraph (II) in which the copy is to be supplied; and (B) as soon as practicable, supply the copy – (I) in the form specified in the response, if any, to the notice referred to in subparagraph (A); (II) if there is no such response within the period specified in subparagraph (A)(III) [14 days], supply the copy in any one of the forms referred to in subparagraph (A)(II) as the data user thinks fit.
See Article 12(5) in section 5.1. above.	Section 20: (1) A data user shall refuse to comply with a data access request – (a) if the data user is not supplied with such information as the data user may reasonably require – (i) in order to satisfy the data user as to the identity of the requestor; (ii) where the requestor purports to be a relevant person, in order to satisfy the data user – (A) as to the identity of the individual in relation to whom the requestor purports to be such a person; and (B) that the requestor is such a person in relation to that individual; (b) subject to subsection (2), if the data user cannot comply with the request without disclosing personal data of which any other individual is the data subject unless the data user is satisfied that the other individual has consented to the disclosure of the data to the requestor; or (c) in any other case, if compliance with the request is for the time being prohibited under this or any other Ordinance. (2) Subsection (1)(b) shall not operate – (a) so that the reference in that subsection to personal data of which any other individual is the data subject includes a reference to information identifying that individual as the source of the personal data to which the data access request concerned relates unless that information names or otherwise explicitly identifies that individual; (b) so as to excuse a data user from complying with the data access request concerned to the extent that the request may be complied with without disclosing the identity of the other individual, whether by the omission of names, or other identifying particulars, or otherwise.

GDPR	PDPO

Differences (cont'd)

(3) A data user may refuse to comply with a data access request if – (a) the request is not in writing in the Chinese or English language;

(b) the data user is not supplied with such information as the data user may reasonably require to locate the personal data to which the request relates;

(c) the request follows two or more similar requests made by – (i) the individual who is the data subject in respect of the personal data to which the request relates; (ii) one or more relevant persons on behalf of that individual; or (iii) any combination of that individual and those relevant persons,

and it is unreasonable in all the circumstances for the data user to comply with the request;

(d) subject to subsection (4), any other data user controls the use of the data in such a way as to prohibit the first-mentioned data user from complying (whether in whole or in part) with the request;

(e) the form in which the request shall be made has been specified under Section 67 and the request is not made in that form;

(ea) the data user is entitled under this or any other Ordinance not to comply with the request; or

(f) in any other case, compliance with the request may for the time being be refused under this Ordinance, whether by virtue of an exemption under Part 8 or otherwise.

(4) Subsection (3)(d) shall not operate so as to excuse a data user from complying with the data access request concerned – (a) in so far as the request relates to Section 18(1)(a), to any extent;

(b) in so far as the request relates to Section 18(1)(b), to any extent that the data user can comply with the request without contravening the prohibition concerned.

5.5. Right not to be subject to discrimination

Like the GDPR, the PDPO does not specifically refer to a right not to be subject to discrimination for exercising rights. However, the PDPO, unlike the GDPR, sets out provisions for matching procedures, including requirements to request to conduct a matching procedure.

GDPR	PDPO

Similarities

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

Differences

GDPR	PDPO
Article 22(1): The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her. [Article 22 goes on to detail this right, including exceptions]	Sections 30-32 of the PDPO regulate 'matching procedures.' Section 2(1): 'matching procedure' means any procedure whereby personal data collected for one or more purposes in respect of 10 or more data subjects is compared (except by manual means) with personal data collected for any other purpose in respect of those data subjects where the comparison – (a) is (whether in whole or in part) for the purpose of producing or verifying data that; or (b) produces or verifies data in respect of which it is reasonable to believe that it is practicable that the data, may be used (whether immediately or at any subsequent time) for the purpose of taking adverse action against any of those data subjects.

5.6. Right to data portability

Inconsistent

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

GDPR	PDPO
Differences	
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 PDPO does not explicitly refer to this right.
See Article 12(1) in section 5.1.	The PDPO does not explicitly refer to this right.
See Article 12(5) in section 5.1. above.	The PDPO does not explicitly refer to this right.
See Article 12(3) in section 5.1. above.	The PDPO does not explicitly refer to this right.
See Article 20(1) above.	The PDPO does not explicitly refer to this right.
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 PDPO does not explicitly refer to this right.
See Article 20(2) above.	The PDPO does not explicitly refer to this right.
See Article 12(5) in section 6.1. above.	The PDPO does not explicitly refer to this right.

6. Enforcement

Fairly inconsistent

6.1. Monetary penalties

Both the GDPR and PDPO provide for monetary penalties and other enforcement actions. Unlike the GDPR, however, the PDPO also provides for imprisonment and sets out several mitigating reasons that may result in a complaint not being investigated. The PDPO also sets out significantly smaller fines than the GDPR.

GDPR	PDPO
Similarities	
The GDPR provides for monetary penalties.	The PDPO provides for monetary penalties.
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.	The PDPO provides the PCPD with the authority to issue enforcement notices (Section 50). Failure to comply with an enforcement notice may result in monetary penalties or imprisonment (Section 50A).
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).	The maximum monetary penalty under the PDPO is HKD 1 million (approx. €106,000). This maximum penalty may be issued for violations of certain direct marketing and disclosure provision.

GDPR	PDPO

Differences (cont'd)

GDPR	PDPO
(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.	
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 PDPO does not provide sanctions in the form of a 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:	Section 50(2): In deciding whether to serve an enforcement notice the Commissioner shall consider whether the contravention to which the notice relates has caused or is likely to cause damage or distress to any individual who is the data subject of any personal data to which the contravention relates.
(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;	Section 50A(2): In any proceedings for an offence under subsection (1), it is a defence for the data user charged to show that the data user exercised all due diligence to comply with the enforcement notice.
(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;	Section 39: (1) Notwithstanding the generality of the powers conferred on the Commissioner by this Ordinance, the Commissioner may refuse to carry out or decide to terminate an investigation initiated by a complaint if – (a) the complainant (or, if the complainant is a relevant person, the individual in respect of whom the complainant is such a person) has had actual knowledge of the act or practice specified in the complaint for more than two years immediately preceding the date on which the Commissioner received the complaint, unless the Commissioner is satisfied that in all the circumstances of the case it is proper to carry out or not to terminate, as the case may be, the investigation;
(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;	(b) the complaint is made anonymously;
(f) the degree of cooperation with the supervisory authority, in order to remedy the infringement and mitigate the possible adverse effects of the infringement;	(c) the complainant cannot be identified or traced;
(g) the categories of personal data affected by the infringement;	(d) none of the following conditions is fulfilled in respect of the act or practice specified in the complaint –
(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;	

GDPR | PDPO

Differences (cont'd)

GDPR	PDPO
(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;	(i) either – (A) the complainant (or, if the complainant is a relevant person, the individual in respect of whom the complainant is such a person) was resident in Hong Kong; or (B) the relevant data user was able to control, in or from Hong Kong, the collection, holding, processing or use of the personal data concerned, at any time the act or practice was done or engaged in, as the case may be;
(j) adherence to approved codes of conduct pursuant to Article 40 or approved certification mechanisms pursuant to Article 42; and	(ii) the complainant (or, if the complainant is a relevant person, the individual in respect of whom the complainant is such a person) was in Hong Kong at any time the act or practice was done or engaged in, as the case may be;
(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.	(iii) in the opinion of the Commissioner, the act or practice done or engaged in, as the case may be, may prejudice the enforcement of any right, or the exercise of any privilege, acquired or accrued in Hong Kong by the complainant (or, if the complainant is a relevant person, the individual in respect of whom the complainant is such a person); or
	(e) the Commissioner is satisfied that the relevant data user has not been a data user for a period of not less than two years immediately preceding the date on which the Commissioner received the complaint.
	(2) The Commissioner may refuse to carry out or decide to terminate an investigation initiated by a complaint if he is of the opinion that, having regard to all the circumstances of the case – (a) the complaint, or a complaint of a substantially similar nature, has previously initiated an investigation as a result of which the Commissioner was of the opinion that there had been no contravention of a requirement under this Ordinance;
	(b) the act or practice specified in the complaint is trivial;
	(c) the complaint is frivolous or vexatious or is not made in good faith;
	(ca) the primary subject matter of the complaint, as shown by the act or practice specified in it, is not related to privacy of individuals in relation to personal data; or
	(d) any investigation or further investigation is for any other reason unnecessary.

GDPR	PDPO
Differences (cont'd)	
Not applicable.	The PDPO provides for a sanction of imprisonment in several instances. The maximum period of imprisonment is for five years, for violations of certain direct marketing and disclosure provisions.
Not applicable.	The PDPO does not refer to DPOs. However, sanctions are applicable to persons.

6.2. Supervisory authority

The GDPR and the PDPO establish data protection authorities and provide them with investigatory, corrective and advisory powers. Although the tasks and powers of these authorities vary in the particulars, there are general similarities.

GDPR	PDPO
Similarities	
Article 51(1) of the GDPR: Each Member State shall provide for one or more independent public authorities to be responsible for monitoring the application of this Regulation, in order to protect the fundamental rights and freedoms of natural persons in relation to processing and to facilitate the free flow of personal data within the Union ('supervisory authority').	Section 5(1) of the PDPO: For the purposes of this Ordinance, there is hereby established an office by the name of the Privacy Commissioner for Personal Data.
Article 58(1): Each supervisory authority shall have all of the following investigative powers: (a) to order the controller and the processor, and, where applicable, the controller's or the processor's representative to provide any information it requires for the performance of its tasks; (b) to carry out investigations in the form of data protection audits; (c) to carry out a review on certifications issued pursuant to Article 42(7); (d) to notify the controller or the processor of an alleged infringement of this Regulation; (e) to obtain, from the controller and the processor, access to all personal data and to all information necessary for the performance of its tasks; (f) to obtain access to any premises of the controller and the processor, including to any data processing equipment and means, in accordance with Union or Member State procedural law.	Section 36: Without prejudice to the generality of Section 38, the Commissioner may carry out an inspection of – (a) any personal data system used by a data user; or (b) any personal data system used by a data user belonging to a class of data users, for the purposes of ascertaining information to assist the Commissioner in making recommendations – (i) to – (A) where paragraph (a) is applicable, the relevant data user; (B) where paragraph (b) is applicable, the class of data users to which the relevant data user belongs; and (ii) relating to the promotion of compliance with the provisions of this Ordinance, in particular the data protection principles, by the relevant data user, or the class of data users to which the relevant data user belongs, as the case may be. Section 38: Where the Commissioner – (a) receives a complaint; or (b) has reasonable grounds to believe that an act or practice – (i) has been done or engaged in, or is being done or engaged in, as the case may be, by a data user; (ii) relates to personal data; and (iii) may be a contravention of a requirement under this Ordinance, then –

GDPR	PDPO

Differences (cont'd)

GDPR	PDPO
	(i) where paragraph (a) is applicable, the Commissioner shall, subject to Section 39, carry out an investigation in relation to the relevant data user to ascertain whether the act or practice specified in the complaint is a contravention of a requirement under this Ordinance; (ii) where paragraph (b) is applicable, the Commissioner may carry out an investigation in relation to the relevant data user to ascertain whether the act or practice referred to in that paragraph is a contravention of a requirement under this Ordinance. [Note: Sections 42-49 further detail the processes of investigations, including the capacity for the PCPD to enter premises.]
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;	Section 50: (1) If, following the completion of an investigation, the Commissioner is of the opinion that the relevant data user is contravening or has contravened a requirement under this Ordinance, the Commissioner may serve on the data user a notice in writing, directing the data user to remedy and, if appropriate, prevent any recurrence of the contravention. (1A) An enforcement notice under subsection (1) must – (a) state that the Commissioner is of the opinion referred to in subsection (1) and the reason for that opinion; (b) specify – (i) the requirement which, in the opinion of the Commissioner, is being or has been contravened; and (ii) the act or omission that constitutes the contravention; (c) specify the steps that the data user must take (including ceasing any act or practice) to remedy and, if appropriate, prevent any recurrence of the contravention; (d) specify the date on or before which the steps must be taken; and (e) be accompanied by a copy of this Section. (1B) The date specified in subsection (1A)(d) must be a date which is not earlier than the expiry of the period specified in subsection (7) within which an appeal against the notice may be made.

GDPR | PDPO

Differences (cont'd)

GDPR	PDPO
(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.	(1B) The date specified in subsection (1A)(d) must be a date which is not earlier than the expiry of the period specified in subsection (7) within which an appeal against the notice may be made. (2) In deciding whether to serve an enforcement notice the Commissioner shall consider whether the contravention to which the notice relates has caused or is likely to cause damage or distress to any individual who is the data subject of any personal data to which the contravention relates. (3) The steps specified in an enforcement notice to remedy and, if appropriate, prevent any recurrence of any contravention to which the notice relates may be framed – (a) to any extent by reference to any approved code of practice; and (b) so as to afford the relevant data user a choice between different ways of remedying and, if appropriate, preventing any recurrence of the contravention. (4) Subject to subsection (5), the period specified in an enforcement notice for taking the steps specified in it shall not expire before the end of the period specified in subsection (7) within which an appeal against the notice may be made and, if such an appeal is made, those steps need not be taken pending the determination or withdrawal of the appeal. (5) If the Commissioner is of the opinion that by reason of special circumstances the steps specified in an enforcement notice should be taken as a matter of urgency – (a) he may include a statement to that effect in the notice together with the reasons why he is of that opinion; (b) where such a statement is so included, subsection (4) shall not apply but the notice shall not require those steps to be taken before the end of the period of seven years beginning with the date on which the notice was served. (6) The Commissioner may cancel an enforcement notice by notice in writing served on the relevant data user. (7) An appeal may be made to the Administrative Appeals Board against an enforcement notice by the relevant data user not later than 14 days after the notice was served.

GDPR	PDPO

Differences (cont'd)

GDPR	PDPO
	(8) Where the Commissioner – (a) forms an opinion referred to in subsection (1) in respect of the relevant data user at any time before the completion of an investigation; and (b) is also of the opinion that, by reason of special circumstances, an enforcement notice should be served on the relevant data user as a matter of urgency, he may so serve such notice notwithstanding that the investigation has not been completed and, in any such case – (i) the Commissioner shall, without prejudice to any other matters to be included in such notice, specify in the notice the reasons as to why he is of the opinion referred to in paragraph (b); and (ii) the other provisions of this Ordinance (including this Section) shall be construed accordingly.
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);	The PCPD is provided with various authorisation and advisory powers within the PDPO. Notably, Section 12 of the PDPO establishes the PCPD's authority to issue codes of practice.

GDPR	PDPO

Differences (cont'd)

GDPR	PDPO
(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 57(1): Without prejudice to other tasks set out under this Regulation, each supervisory authority shall on its territory: (a) monitor and enforce the application of this Regulation; (b) promote public awareness and understanding of the risks, rules, safeguards and rights in relation to processing. Activities addressed specifically to children shall receive specific attention; (c) advise, in accordance with Member State law, the national parliament, the government, and other institutions and bodies on legislative and administrative measures relating to the protection of natural persons' rights and freedoms with regard to processing; (d) promote the awareness of controllers and processors of their obligations under this Regulation; (e) upon request, provide information to any data subject concerning the exercise of their rights under this Regulation and, if appropriate, cooperate with the supervisory authorities in other Member States to that end; (f) handle complaints lodged by a data subject, or by a body, organisation or association in accordance with Article 80, and investigate, to the extent appropriate, the subject matter of the complaint and inform the complainant of the progress and the outcome of the investigation within a reasonable period, in particular if further investigation or coordination with another supervisory authority is necessary; (g) cooperate with, including sharing information and provide mutual assistance to, other supervisory authorities with a view to ensuring the consistency of application and enforcement of this Regulation;	Section 8: (1) The Commissioner shall – (a) monitor and supervise compliance with the provisions of this Ordinance; (b) promote and assist bodies representing data users to prepare, for the purposes of Section 12, codes of practice for guidance in complying with the provisions of this Ordinance, in particular the data protection principles; (c) promote awareness and understanding of, and compliance with, the provisions of this Ordinance, in particular the data protection principles; (d) examine any proposed legislation (including subsidiary legislation) that the Commissioner considers may affect the privacy of individuals in relation to personal data and report the results of the examination to the person proposing the legislation; (e) carry out inspections, including inspections of any personal data systems used by data users which are departments of the Government or statutory corporations; (f) for the better performance of his other functions, undertake research into, and monitor developments in, the processing of data and information technology in order to take account of any likely adverse effects such developments may have on the privacy of individuals in relation to personal data; (g) liaise and co-operate with any person in any place outside Hong Kong – (i) performing in that place any functions which, in the opinion of the Commissioner, are similar (whether in whole or in part) to any of the Commissioner's functions under this Ordinance; and (ii) in respect of matters of mutual interest concerning the privacy of individuals in relation to personal data; and

GDPR	PDPO

Differences (cont'd)

GDPR	PDPO
(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); (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;	(h) perform such other functions as are imposed on him under this Ordinance or any other enactment. (2) The Commissioner may do all such things as are necessary for, or incidental or conducive to, the better performance of his functions and in particular but without prejudice to the generality of the foregoing, may – (a) acquire and hold property of any description if in the opinion of the Commissioner such property is necessary for – (i) the accommodation of the Commissioner or of any prescribed officer; or (ii) the performance of any function which the Commissioner may perform, and, subject to the terms and conditions upon which such property is held, dispose of it; (b) enter into, carry out, assign or accept the assignment of, vary or rescind, any contract, agreement or other obligation; (c) undertake and execute any lawful trust which has as an object the furtherance of any function which the Commissioner is required or is permitted by this Ordinance to perform or any other similar object; (d) accept gifts and donations, whether subject to any trust or not; (e) with the prior approval of the Chief Executive, become a member of or affiliate to any international body concerned with (whether in whole or in part) the privacy of individuals in relation to personal data; (ea) carry out promotional or educational activities or services; and (f) exercise such other powers as are conferred on him under this Ordinance or any other enactment.

GDPR	PDPO

Differences (cont'd)

GDPR	PDPO
(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.	(2A) The Commissioner may impose reasonable charges for any promotional or educational activities or services carried out, or any promotional or educational publications or materials made available, by the Commissioner in the course of the performance of the Commissioner's functions under this Ordinance. (3) The Commissioner may make and execute any document in the performance of his functions or the exercise of his powers or in connection with any matter reasonably incidental to or consequential upon the performance of his functions or the exercise of his powers. (4) Any document purporting to be executed under the seal of the Commissioner shall be admitted in evidence and shall, in the absence of evidence to the contrary, be deemed to have been duly executed. (5) The Commissioner may from time to time cause to be prepared and published by notice in the Gazette, for the guidance of data users and data subjects, guidelines not inconsistent with this Ordinance, indicating the manner in which he proposes to perform any of his functions, or exercise any of his powers, under this Ordinance.
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.	Section 4(4): The Commissioner shall, as soon as practicable and in any case not later than nine months after the expiry of a financial year (or such further period as the Chief Secretary for Administration allows), furnish – (a) a report on the activities of the Commissioner during that year including a general survey of developments, during that year, in respect of matters falling within the scope of the Commissioner's functions; (b) a copy of the statement of accounts required under subsection (2); and (c) the auditor's report on the statement, to the Chief Secretary for Administration who shall cause the same to be tabled in the Legislative Council.

6.3. Civil remedies for individuals

Fairly consistent

Both the GDPR and the PDPO establish grounds for compensation for both material and non-material damages. Similarly, neither piece of legislation specifies how the amount of damages will be calculated. The GDPR and the PDPO differ, nevertheless, in regard to mandates for representation, processor liabilities, and exceptions from such compensation.

GDPR	PDPO

Similarities

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.

Section 66(1): Subject to subsection (4), an individual who suffers damage by reason of a contravention –

(a) of a requirement under this Ordinance;

(b) by a data user; and

(c) which relates, whether in whole or in part, to personal data of which that individual is the data subject,

shall be entitled to compensation from that data user for that damage.

Article 82(1): Any person who has suffered material or non-material damage as a result of an infringement of this Regulation shall have the right to receive compensation from the controller or processor for the damage suffered.

Section 66(2): For the avoidance of doubt, it is hereby declared that damage referred to in subsection (1) may be or include injury to feelings.

Differences

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.

Section 66B(1): A person who may institute proceedings to seek compensation under Section 66 may make an application to the Commissioner for assistance in respect of those proceedings.

GDPR	PDPO

Differences (cont'd)

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 PDPO does not explicitly refer to this matter.

Article 82(3): A controller or processor shall be exempt from liability under paragraph 2 if it proves that it is not in any way responsible for the event giving rise to the damage.

The PDPO does not provide explicit exceptions from compensation, however it does set out the following:

Section 66: (3) In any proceedings brought against any person by virtue of this Section it shall be a defence to show that –
(a) he had taken such care as in all the circumstances was reasonably required to avoid the contravention concerned; or

(b) in any case where the contravention concerned occurred because the personal data concerned was inaccurate, the accurately record data received or obtained by the data user concerned from the data subject or a third party.

(4) Where an individual suffers damage referred to in subsection (1) by reason of a contravention referred to in that subsection which occurred because the personal data concerned was inaccurate, then no compensation shall be payable under that subsection in respect of so much of that damage that has occurred at any time before the expiration of one year immediately following the day on which this Section commences.