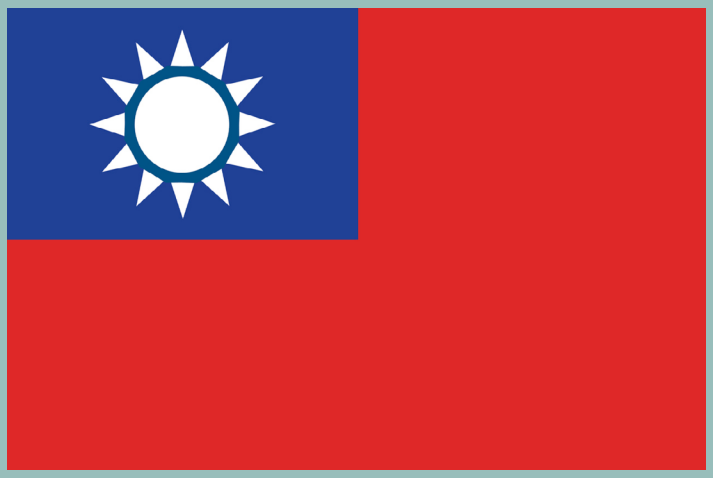


# Comparing privacy laws:
# GDPR v. PDPA

OneTrust DataGuidance™
REGULATORY RESEARCH SOFTWARE

## About the authors

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

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

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

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



# Table of contents

Introduction 5

1. Scope
1.1. Personal scope 7
1.2. Territorial scope 9
1.3. Material scope 10

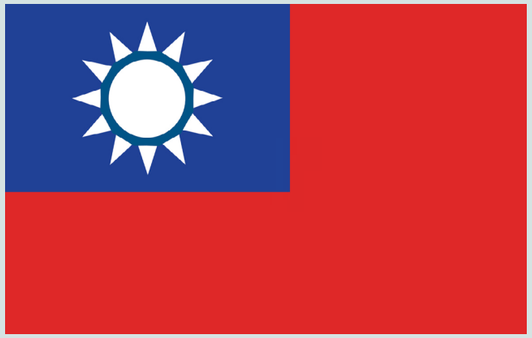
2. Key definitions
2.1. Personal data 12
2.2. Pseudonymisation 13
2.3. Controller and processors 14
2.4. Children 16
2.5. Research 17

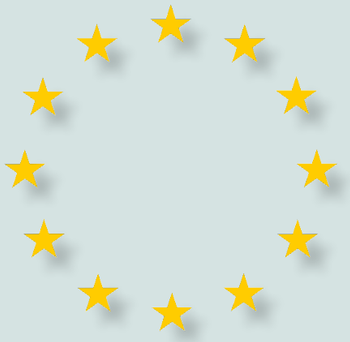
3. Legal basis 19

4. Controller and processor obligations
4.1. Data transfers 21
4.2. Data processing records 23
4.3. Data protection impact assessment 26
4.4. Data protection officer appointment 29
4.5. Data security and data breaches 31
4.6. Accountability 33

5. Individuals' rights
5.1. Right to erasure 34
5.2. Right to be informed 38
5.3. Right to object 42
5.4. Right of access 45
5.5. Right not to be subject to discrimination 47
5.6. Right to data portability 48

6. Enforcement
6.1. Monetary penalties 49
6.2. Supervisory authority 52
6.3. Civil remedies for individuals 58





# Introduction

The General Data Protection Regulation (Regulation (EU) 2016/679) ('GDPR'), which came into effect on 25 May 2018, governs the protection of personal data in EU and EEA Member States. The Personal Data Protection Act 2010 (as amended in 2015) ('PDPA') which took effect on 15 March 2016, and the Enforcement Rules of the Personal Data Protection Act ('Enforcement Rules') are the primary legislation governing the collection, processing, or use of personal data in Taiwan. The National Development Council ('NDC') is the national data protection regulator adopting its functions from the Ministry of Justice. The NDC has corrective and investigatory powers including the issuance of fines and corrective orders and can conduct on-site inspections of certain non-government agencies.

In general terms, there are broad similarities between the PDPA and the GDPR, for instance both legislations address matters such as data subject rights, provide lawful bases for data processing, as well as restrictions on international data transfers. However, the content of these provisions often differs significantly. In addition, the GDPR and the PDPA diverge in their regulation of data processors, protection of children, and responsibilities of data controllers as well as government and non-government agencies, respectively. Specifically, the obligations imposed on government and non-government agencies in the PDPA are less extensive than those provided in the GDPR, and omit obligations including in relation to conducting Data Protection Impact Assessments ('DPIA'), data breach notifications, mandatory data protection officer ('DPO') appointment, and record-keeping.

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

## Structure and overview of the Guide

This Guide provides a comparison of the two legislative frameworks on the following key provisions:

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

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

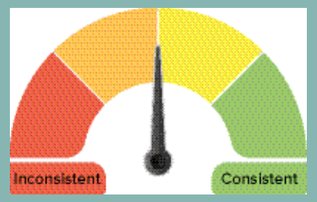
### Key for giving the consistency rate

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

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

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

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




## Usage of the Guide

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



# 1. Scope

Fairly consistent

## 1.1. Personal scope

Although the GDPR and PDPA both regulate the processing of personal information by private organisations as well as public bodies, and only apply to living persons, there are notable differences between the two legislations. In particular, the GDPR provides a clear definition of a data processor and its associated responsibilities, whereas the PDPA does not reference data processors.

| GDPR | PDPA |
|---|---|
| **Similarities** | |
| Article 4(7): 'controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law. | The PDPA applies to 'government agencies' and 'non-government agencies'.<br><br>Article 2(7) of the PDPA: 'government agency' refers to a central or local government agency or administrative entity authorised to exercise public authority.<br><br>Article 2(8) of the PDPA: 'non-government agency' refers to a natural person, legal person or group other than those stated in the preceding subparagraph. |
| Article 4(1): 'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. | Article 2(9) of the PDPA: 'data subject' refers to an individual whose personal data is collected, processed, or used. |
| Article 4(7): 'controller' means the natural or legal person, public authority, agency or other body. | Article 2(7) of the PDPA: 'government agency' refers to a central or local government agency or administrative entity authorised to exercise public authority. |
| 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.<br><br>Regarding the place of residence see Recital 14 above. | Article 51 of the PDPA: The PDPA also applies to the government and the non-government agencies outside the territory of the Republic of China (Taiwan) when they collect, process, or use the personal data of Taiwan nationals.<br><br>Regarding the place of residence see Article 51 above. |

| GDPR | PDPA |
|---|---|
| **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. | Article 4 of the PDPA: Whoever is commissioned by a government agency or non-government agency to collect, process, or use personal data shall be deemed to be acting on behalf of the commissioning agency to the extent that the PDPA applies. |
| 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. | Article 2 of the Enforcement Rules: A 'person' or 'individual', as referred to under the PDPA, shall mean a living natural person. |

**Fairly consistent**

## 1.2. Territorial scope

Similar to the GDPR, the PDPA has extraterritorial application, applying to government and non-government agencies that operate outside of Taiwan when they collect, process, or use the personal data of Taiwanese nationals. However, the PDPA does not explicitly regulate goods and services or monitoring from abroad, nor does it explicitly address government and non-government agencies being established within Taiwan.

| GDPR | PDPA |
|---|---|
| **Similarities** | |
| Article 3: This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not. | Article 51 of the PDPA: The PDPA also applies to the government and the non-government agencies outside the territory of the Republic of China (Taiwan) when they collect, process, or use the personal data of the Taiwan nationals. |

# 1.3. Material scope


The PDPA and the GDPR adopt similar concepts of personal data and data processing. In addition, both pieces of legislation provide general exceptions for the processing of personal data for purely personal or household activities. However, the PDPA does not directly address anonymous data, nor does it explicitly define special categories of data, although it does afford enhanced protection to certain types of personal data including healthcare, genetics, physical examination, and criminal records.

| GDPR | PDPA |
|---|---|
| **Similarities** | |
| Article 4(1): 'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. | Article 2(1): 'personal data' refers to a natural person's name, date of birth, ID Card number, passport number, features, fingerprints, marital status, family information, education background, occupation, medical records, healthcare data, genetic data, data concerning a person's sex life, records of physical examination, criminal records, contact information, financial conditions, data concerning a person's social activities and any other information that may be used to directly or indirectly identify a natural person. |
| Article 4(2): 'processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. | Article 2(4): 'processing' refers to the act of recording, inputting, storing, compiling/editing, correcting, duplicating, retrieving, deleting, outputting, connecting or internally transferring data for the purpose of establishing or using a personal data file. |
| Article 2(2): This Regulation does not apply to the processing of personal data:<br><br>(a) in the course of an activity which falls outside the scope of Union law;<br><br>(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<br><br>(c) by a natural person in the course of a purely personal or household activity. | Article 51(1)(2) of the PDPA: The PDPA does not apply to the following circumstances: where personal data is being collected, processed, or used by a natural person purely for purposes of personal or household activities; or where audio-visual data is collected, processed, or used in public places or public activities and not connected to other personal data. |



| GDPR | PDPA |
|---|---|
| **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 PDPA and Enforcement Rules do not explicitly refer special categories of personal data. However, Article 6 of the PDPA provides data pertaining to a natural person's medical records, healthcare, genetics, sex life, physical examination and criminal records shall not be collected unless certain exceptions apply.<br><br>Article 4 of the Enforcement Rules provides further information regarding the abovementioned categories of data. |
| Recital 26: The principles of data protection should not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable. | The PDPA and Enforcement Rules do not explicitly refer to anonymised data. |
| Article 4(5): 'pseudonymisation' means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person. | Article 17 of the Enforcement Rules: 'data that may not lead to the identification of a specific data subject'[...] shall mean personal data replaced with codes, deleted data subject's name, partially concealed, or processed via other means to the extent that the data subject may not be directly identified. |
| Article 2(1): This Regulation applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system. | Article 2(4) of the PDPA: 'processing' refers to [...] internally transferring data for the purpose of establishing or using a personal data file.<br><br>Article 2(2) of the PDPA: Personal data file refers to the collection of personal data structured to facilitate data retrieval and management by automated or non-automated means. |

# 2. Key definitions

## 2.1. Personal data


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

| GDPR | PDPA |
|---|---|

### Similarities

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

Article 2(1)of the PDPA: 'personal data' refers to a natural person's name, date of birth, ID Card number, passport number, features, fingerprints, marital status, family information, education background, occupation, medical records, healthcare data, genetic data, data concerning a person's sex life, records of physical examination, criminal records, contact information, financial conditions, data concerning a person's social activities and any other information that may be used to directly or indirectly identify a natural person.

### 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.

Neither the PDPA nor the Enforcement Rules explicitly refer special categories of personal data. However, Article 6 of the PDPA provides data pertaining to a natural person's medical records, healthcare, genetics, sex life, physical examination and criminal records shall not be collected unless certain exceptions apply.

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

The PDPA and Enforcement Rules do not explicitly refer to online identifiers.



## 2.2. Pseudonymisation


The GDPR defines pseudonymised data, whereas the Enforcement Rules refer to 'data that may not lead to the identification of a specific data subject', both concepts ensure that personal data cannot directly identify the natural person. The PDPA does not directly define or refer to anonymisation.

| GDPR | PDPA |
|---|---|

### Similarities

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.

Article 17 of the Enforcement Rules: 'data that may not lead to the identification of a specific data subject'[...] shall mean personal data replaced with codes, deleted data subject's name, partially concealed, or processed via other means to the extent that the data subject may not be directly identified.

### Differences

Recital 26: 'anonymous information' is information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable.

The PDPA and the Enforcement Rules do not explicitly refer to anonymised data.

# 2.3. Controllers and processors

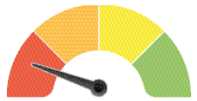

The GDPR defines the concepts of 'data controllers' and 'data processors,' whereas the PDPA defines the broader concept of 'non-government' and 'government' agencies. Moreover, the PDPA and its Enforcement Rules require the assignment of dedicated personnel to implement security and maintenance measures, which is much narrower than the concept of a DPO under the GDPR. In addition, the PDPA does not directly define data processors, nor does it directly address controller and processor responsibilities as provided for under the GDPR, such as DPIA, or controller/processor contracts.

| GDPR | PDPA |
|---|---|
| **Differences** | |
| Article 4(7): 'controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law. | The PDPA applies to 'government agencies' and 'non-government agencies'.<br><br>Article 2(7) of the PDPA: 'government agency' refers to a central or local government agency or administrative entity authorised to exercise public authority.<br><br>Article 2(8) of the PDPA: 'non-government agency' refers to a natural person, legal person or group other than those stated in the preceding subparagraph. |
| Article 4(8): 'processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller. | Article 4 of the PDPA: 'Whoever is commissioned by a government agency or non-government agency to collect, process or use personal data shall be deemed to be acting on behalf of the commissioning agency to the extent that the PDPA applies'. |
| 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.] | The PDPA and the Enforcement Rules do not refer to controller and processor contracts. |
| DPIA is not specifically defined, however Article 35 sets out requirements for DPIAs (see section 5.3. for further information). | The PDPA and the Enforcement Rules do not define DPIAs. However, Article 12 of the Enforcement Rules outline the establishment of a mechanism of risk assessments as a proper security and maintenance measure. |



| GDPR | PDPA |
|---|---|
| **Differences (cont'd)** | |
| DPO is not specifically defined, however Article 37 sets out requirements related to DPOs (see section 5.4. for further information). | The PDPA and the Enforcement Rules do not refer to DPOs.<br><br>However, Article 18 of the PDPA requires assignment of a dedicated personnel to implement security and maintenance measures to prevent the personal data from being stolen, altered, damaged, destroyed or disclosed. |

## 2.4. Children



Inconsistent

Unlike the GDPR, the PDPA does not address the processing of children's data nor does it provide additional requirements for said processing.

| GDPR | PDPA |
|---|---|

### Differences

| GDPR | PDPA |
|---|---|
| The GDPR does not specifically define 'child'. However, Article 8(1) provides: Where point (a) of Article 6(1) applies, in relation to the offer of information society services directly to a child, the processing of the personal data of a child shall be lawful where the child is at least 16 years old. Where the child is below the age of 16 years, such processing shall be lawful only if and to the extent that consent is given or authorised by the holder of parental responsibility over the child. Member States may provide by law for a lower age for those purposes provided that such lower age is not below 13 years. | The PDPA and the Enforcement Rules do not address the processing of children's data. |
| Article 8(2): The controller shall make reasonable efforts to verify in such cases that consent is given or authorised by the holder of parental responsibility over the child, taking into consideration available technology. | The PDPA and the Enforcement Rules do not refer to consent for the processing of children's data. |
| Recital 58: Given that children merit specific protection, any information and communication, where processing is addressed to a child, should be in such a clear and plain language that the child can easily understand. | The PDPA and the Enforcement Rules do not provide specific requirements in relation to the processing of children's data. |



## 2.5. Research

Fairly consistent

The PDPA provides exemptions to data processing for statistical gathering and academic research, whereas the GDPR provides exemptions to data processing for scientific and historical research. Both pieces of legislation permit further processing, require the implementation of appropriate safeguards, and place limits on data subject right on this basis. Unlike the GDPR, however, the PDPA does not provide a definition of statistic gathering and academic research.

| GDPR | PDPA |
|---|---|

### Similarities

| GDPR | PDPA |
|---|---|
| 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'). | Articles 16(5) and 20(5) of the PDPA: Except for the personal data specified under Paragraph 1, Article 6, a government agency or non-government agency shall use personal data only within the necessary scope of its statutory duties and for the specific purpose of collection; the use of personal data for another purpose shall be only on any of the following bases [...] where it is necessary for statistics gathering or academic research by a government agency or an academic institution for public interests; provided that such data, as processed by the data provider or as disclosed by the data collector, may not lead to the identification of a specific data subject. |
| 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. | See Articles 16(5) and 20(5) above. |
| 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. | Article 9(4) of the PDPA: The obligation to inform as prescribed in Paragraph 9(1) may be exempt under any of the following circumstances [...] where it is necessary for statistics gathering or academic research in pursuit of public interests, provided that such data, as processed by the data provider or as disclosed by the data collector, may not lead to the identification of a specific data subject. |

| GDPR | PDPA |
|---|---|

## Differences

Recital 159: Where personal data are processed for scientific research purposes, this Regulation should also apply to that processing. For the purposes of this Regulation, the processing of personal data for scientific research purposes should be interpreted in a broad manner including for example technological development and demonstration, fundamental research, applied research and privately funded research.

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

The PDPA applies and refers to the processing of personal data for statistics gathering or academic research but does not provide definitions thereof.





# 3. Legal basis

**Fairly inconsistent**

The PDPA and GDPR set out very similar grounds for the processing of personal data by non - government agencies and data controllers, respectively. Moreover, both pieces of legislation provide enhanced protection for certain types of data, under the GDPR this is referred to as special categories of personal data. However, the PDPA does not address the withdrawal of consent, nor does it provide exceptions for data processed for journalistic/artistic purposes.

| GDPR | PDPA |
|---|---|

## Similarities

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

Article 6 of the PDPA outlines specific requirements for the processing of certain types of data including medical records, healthcare, genetics, sex life, physical examination and criminal records.

## Differences

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

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

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

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

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

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

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

Article 15 of the PDPA: Except for the personal data specified under Paragraph 1, Article 6, the collection or processing of personal data by a government agency shall be for specific purposes and on one of the following bases:

- where it is within the necessary scope to perform its statutory duties;
- where consent has been given by the data subject; or
- where the rights and interests of the data subject will not be infringed upon.

Article 19 of the PDPA: Except for the personal data specified under Paragraph 1, Article 6, the collection or processing of personal data by a non-government agency shall be for specific purposes and on one of the following bases:

- where it is expressly required by law;
- where there is a contractual or quasi-contractual relationship between the non-government agency and the data subject, and proper security measures have been adopted to ensure the security of the personal data;
- where the personal data has been disclosed to the public by the data subject or has been made public lawfully;
- where it is necessary for statistics gathering or academic research by an academic institution in pursuit of public interests, provided that such data, as processed by the data provider or as disclosed by the data collector, may not lead to the identification of a specific data subject;

| GDPR | PDPA |
|---|---|
| **Differences (cont'd)** | |
| | • where consent has been given by the data subject;<br>• where it is necessary for furthering public interest;<br>• where the personal data is obtained from publicly available sources unless the data subject has an overriding interest in prohibiting the processing or use of such personal data; or<br>• where the rights and interests of the data subject will not be infringed upon. |
| 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.<br><br>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. | The PDPA and the Enforcement Rules do not address the withdrawal of consent. |
| Article 85(1): Member States shall by law reconcile the right to the protection of personal data pursuant to this Regulation with the right to freedom of expression and information, including processing for journalistic purposes and the purposes of academic, artistic or literary expression. | The PDPA does not directly address journalistic and/or artistic purposes as a legal basis. Article 9 of the PDPA briefly refers to journalism in the context of data subject rights. |





# 4. Controller and processor obligations

**Fairly inconsistent**

## 4.1. Data transfers

The PDPA provides for a similar notion of adequate protection to the GDPR. However, the PDPA outlines instances where central authorities may restrict international data transfers, whereas the GDPR sets out a range of mechanisms to enable international transfers of data, such as adequacy, standard contractual clauses ('SCCs'), and Binding Corporate Rules ('BCR').

| GDPR | PDPA |
|---|---|
| **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. | Article 21 of the PDPA: If a cross-border transfer of personal data is carried out by a non-government agency under any of the following circumstances, the central government authority in charge of the industry concerned may impose restrictions on such transfer [...] where the country receiving the personal data lacks proper regulations on protection of personal data and the data subjects' rights and interests may consequently be harmed. |
| **Differences** | |
| Article 46(1): In the absence of a decision pursuant to Article 45(3), a controller or processor may transfer personal data to a third country or an international organisation only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available.<br><br>(2) The appropriate safeguards referred to in paragraph 1 may be provided for, without requiring any specific authorisation from a supervisory authority, by:<br><br>(a) a legally binding and enforceable instrument between public authorities or bodies;<br><br>(b) binding corporate rules in accordance with Article 47;<br><br>(c) standard data protection clauses adopted by the Commission in accordance with the examination procedure referred to in Article 93(2); | Article 21 of the PDPA: If a cross-border transfer of personal data is carried out by a non-government agency under any of the following circumstances, the central government authority in charge of the industry concerned may impose restrictions on such transfer:<br><br>• where major national interests are involved;<br>• where an international treaty or agreement so stipulates;<br>• where the country receiving the personal data lacks proper regulations on protection of personal data and the data subjects' rights and interests may consequently be harmed; or<br>• where the cross-border transfer of the personal data to a third country (territory) is carried out to circumvent the PDPA. |

| GDPR | PDPA |
|---|---|

**Differences (cont'd)**

(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.





## 4.2. Data processing records

**Inconsistent**

While the GDPR requires both data controllers and data processors to maintain data processing records, the PDPA does not provide such an obligation. Instead, the PDPA establishes record keeping as a recommended proper security and maintenance measure.

| GDPR | PDPA |
|---|---|

**Differences**

Article 30(1): Each controller and, where applicable, the controller's representative, shall maintain a record of processing activities under its responsibility. That record shall contain all of the following information:

(a) the name and contact details of the controller and, where applicable, the joint controller, the controller's representative and the data protection officer;

(b) the purposes of the processing;

(c) a description of the categories of data subjects and of the categories of personal data;

(d) the categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organisations;

(e) where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, in the case of transfers referred to in the second subparagraph of Article 49(1), the documentation of suitable safeguards;

(f) where possible, the envisaged time limits for erasure of the different categories of data; and

(g) where possible, a general description of the technical and organisational security measures referred to in Article 32(1).

The PDPA and the Enforcement Rules do not contain specific record-keeping requirements.

However, Article 12 of the Enforcement Rules outlines keeping records, log files, and relevant evidence as proper security and maintenance measures.

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

The PDPA and the Enforcement Rules do not contain specific record-keeping requirements for entities acting on behalf of the commissioning agency.

| GDPR | PDPA |
|---|---|
| **Differences (cont'd)** | |
| processor's representative, and the data protection officer;<br><br>(b) the categories of processing carried out on behalf of each controller;<br><br>(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<br><br>(d) where possible, a general description of the technical and organisational security measures referred to in Article 32(1). | (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.<br><br>The PDPA 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 PDPA and the Enforcement Rules do not contain specific record-keeping requirements. |
| Article 30(4): The controller or the processor and, where applicable, the controller's or the processor's representative, shall make the record available to the supervisory authority on request. | The PDPA and the Enforcement Rules do not contain specific record-keeping requirements. |
| Article 30(5): The obligations referred to in paragraphs 1 and 2 shall not apply to an enterprise or an organisation employing fewer than 250 persons unless the processing it carries out is likely to result in a risk to the rights and freedoms of data subjects, the processing is not occasional, or the processing includes special categories of data as referred to in Article 9(1) or personal data relating to criminal convictions and offences referred to in Article 10. | The PDPA and the Enforcement Rules do not contain specific record-keeping requirements. |





## 4.3. Data protection impact assessment

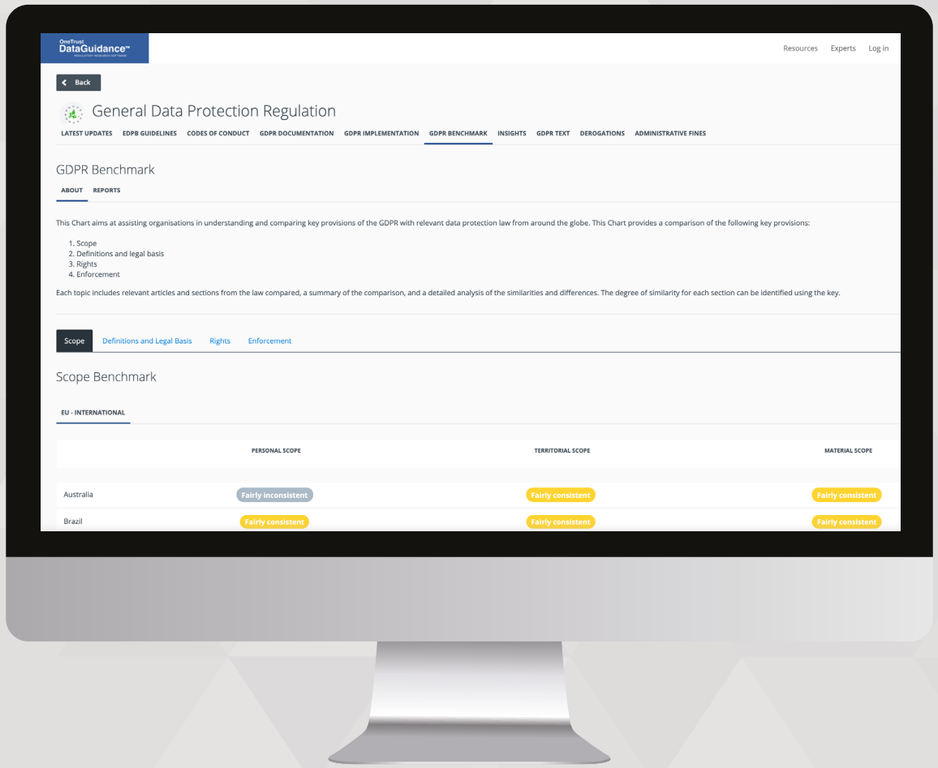

While the GDPR outlines specific requirements for the conducting of DPIAs, the PDPA does not provide such an obligation. Instead, the PDPA recommends the establishment of risk assessments for the purposes of data protection as a proper security and maintenance measure.

| GDPR | PDPA |
|---|---|
| **Similarities** | |
| Article 35(1): Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks.<br><br>[...] (3) A data protection impact assessment referred to in paragraph 1 shall in particular be required in the case of:<br><br>(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;<br><br>(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<br><br>(c) a systematic monitoring of a publicly accessible area on a large scale. | The PDPA and the Enforcement Rules do not contain specific DPIA requirements.<br><br>However, Article 12 of the Enforcement Rules outline the establishment of a mechanism of risk assessments as proper security and maintenance measure. |
| **Differences** | |
| Article 35(7): The assessment shall contain at least:<br><br>(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;<br><br>(b) an assessment of the necessity and proportionality of the processing operations in relation to the purposes; | The PDPA and the Enforcement Rules do not address the content of the risk assessment. |

# Global Regulatory Research Software

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

Monitor regulatory developments, mitigate risk, and achieve global compliance




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

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

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

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

- Scope
- Rights
- Definitions and legal basis
- Enforcement

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

OneTrust
**DataGuidance™**
REGULATORY RESEARCH SOFTWARE

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

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





## 4.4. Data protection officer appointment


Although the PDPA does not provide for the appointment of a DPO, the PDPA and Enforcement Rules provide that government and non-government agencies should assign personnel, in certain circumstances, for the security and maintenance of those files to prevent them from being stolen, altered, damaged, destroyed, or disclosed. Notably, the scope of the assigned personnel is much narrower than that of a DPO under the GDPR.

| GDPR | PDPA |
|---|---|
| **Differences** | |
| Article 39(1): The data protection officer shall have at least the following tasks:<br><br>(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;<br><br>(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;<br><br>(c) to provide advice where requested as regards the data protection impact assessment and monitor its performance pursuant to Article 35;<br><br>(d) to cooperate with the supervisory authority; and<br><br>(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. | There is no explicit requirement to appoint a DPO.<br><br>However, Article 18 of the PDPA states the government agency in possession of personal data files shall assign dedicated personnel to implement security and maintenance measures to prevent the personal data from being stolen, altered, damaged, destroyed or disclosed.<br><br>In addition, Article 12(1) of the Enforcement Rules provides that 'proper security and maintenance measures' may include allocating management personnel and reasonable resources. |
| Article 37(1): The controller and the processor shall designate a data protection officer in any case where:<br><br>(a) the processing is carried out by a public authority or body, except for courts acting in their judicial capacity; | Please see Article 18 above. |

| GDPR | PDPA |
|---|---|

## Similarities (cont'd)

(b) the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale; or

(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.

## Differences

| | |
|---|---|
| Article 37(2): A group of undertakings may appoint a single data protection officer provided that a data protection officer is easily accessible from each establishment. | The PDPA and the Enforcement Rules do not refer to group appointments of dedicated personnel. |
| Article 37(7): The controller or the processor shall publish the contact details of the data protection officer and communicate them to the supervisory authority. | The PDPA and the Enforcement Rules do not require notification of dedicated personnel to the NDC. |
| Article 37(5): The data protection officer shall be designated on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and the ability to fulfil the tasks referred to in Article 39. | The PDPA and the Enforcement Rules do not refer to the qualifications of the dedicated personnel. |





# 4.5. Data security and data breaches

**Fairly inconsistent**

Unlike the GDPR, which requires notification to the relevant supervisory authority, the PDPA does not require government and non-government agencies to notify central government authorities of data breaches. The PDPA does, however, require notification to data subjects if personal data is stolen, disclosed, altered, or otherwise infringed. There are no exceptions provided for data breach notification to data subjects under the PDPA.

| GDPR | PDPA |
|---|---|

## Similarities

| | |
|---|---|
| Article 32(1): Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:<br><br>(a) the pseudonymisation and encryption of personal data;<br><br>(b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;<br><br>(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; and<br><br>(d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing. | Article 12 of the Enforcement Rules: 'Proper security and maintenance measures', as referred in Article 6 of the PDPA, 'security and maintenance measures', as referred to in Article 18 of the PDPA, and 'proper security measures', as referred to in Article 19 and 27 of the PDPA, shall mean the technical or organisational measures taken by a government agency or non-government agency for the purpose of preventing personal data from being stolen, altered, damaged, destroyed or disclosed.<br><br>The measures prescribed in the preceding paragraph may include the following and shall be proportionate to the intended purposes of personal data protection:<br><br>• allocating management personnel and reasonable resources;<br>• defining the scope of personal data;<br>• establishing a mechanism of risk assessment and management of personal data;<br>• establishing a mechanism of preventing, giving notice of, and responding to a data breach;<br>• establishing an internal control procedure for the collection, processing, and use of personal data;<br>• managing data security and personnel;<br>• promoting awareness, education and training;<br>• managing facility security;<br>• establishing an audit mechanism of data security;<br>• keeping records, log files and relevant evidence; and<br>• implementing integrated and persistent improvements on the security and maintenance of personal data. |

| GDPR | PDPA |
|---|---|
| **Differences** | |
| Article 33(1): In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay. | The PDPA and the Enforcement Rules do not explicitly require the notification of data breaches to authority. |
| See Article 33(1) above. | The PDPA and the Enforcement Rules do not address timeframes for breach notification. |
| 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. | Article 12 of the PDPA: If any personal data is stolen, disclosed, altered, or otherwise infringed upon due to a violation of the PDPA by a government or non-government agency, the data subject shall be notified via appropriate means after the relevant facts have been clarified. |
| Article 33(2): The processor shall notify the controller without undue delay after becoming aware of a personal data breach. | The PDPA and the Enforcement Rules do not address notification of data breaches by entities acting on behalf of commissioning agencies. |
| 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:<br><br>(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;<br><br>(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; or<br><br>(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 PDPA and the Enforcement Rules do not explicitly provide exemption to the above notification requirement. | |





## 4.6. Accountability

**Fairly inconsistent**

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

| GDPR | PDPA |
|---|---|
| **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 PDPA. However, the PDPA 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 PDPA 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).<br><br>(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

## 5.1. Right to erasure


The PDPA establishes the right to erasure for data subjects and provides instances when this right can be exercised including situations where the specific purpose of data collection no longer exists or where the collection, processing, or use of personal data is in violation of the PDPA. The bases on which this right can be exercised is much narrower under the PDPA in comparison to the GDPR. In addition, similar to the GDPR, the PDPA outlines the fees, timeframes and publicly available data. However, the PDPA does not specifically address the format of responses by government and non-government agencies, nor provide exceptions to this right.

| GDPR | PDPA |
|---|---|

### Similarities

Article 17(1): The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies:

(a) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;

(b) the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or point (a) of Article 9(2), and where there is no other legal ground for the processing;

(c) the data subject objects to the processing pursuant to Article 21(1) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2);

(d) the personal data have been unlawfully processed;

(e) the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject; or

(f) the personal data have been collected in relation to the offer of information society services referred to in Article 8(1).

Article 3(5) of the PDPA: A data subject shall be able to exercise the following rights with regard to his or her personal data and such rights shall not be waived or limited contractually in advance [...] the right to erase his or her personal data.

Article 11 of the PDPA: When the specific purpose of data collection no longer exists, or upon expiration of the relevant time period, the government or non-government agency shall, on its own initiative or upon the request of the data subject,

erase or cease processing or using the personal data, unless the processing or use is either necessary for the performance of an official or business duty, has been agreed to by the data subject in writing, [...] and erase personal data collected or cease collecting, processing, or using the personal data in the event where the collection, processing or use of the personal data is in violation of the PDPA.





| GDPR | PDPA |
|---|---|

### Similarities (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.

Article 14 of the PDPA: A government or non-government agency may charge a fee to cover necessary costs from those who make an inquiry or request to review or obtain copies of the 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.

Article 13 of the PDPA: [...] where a request is made by a data subject to a government or non-government agency pursuant to Article 11, the agency shall determine whether to accept or reject such request within 30 days; such deadline may be extended by up to 30 days if necessary, and the data subject shall be notified in writing of the reason for the extension.

Article 17(2): Where the controller has made the personal data public and is obliged pursuant to paragraph 1 to erase the personal data, the controller, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform controllers which are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data.

The PDPA and the Enforcement Rules do not refer specifically to publicly available data. However, Article 11 of the PDPA provides that If any failure to correct or supplement any personal data is attributable to a government or non-government agency, the government or non-government agency shall notify the persons who have been provided with such personal data after the correction or supplement is made.

| GDPR | PDPA |
|---|---|
| **Differences** | |
| Article 12(1): The controller shall take appropriate measures to provide any information referred to in Articles 13 and 14 and any communication under Articles 15 to 22 and 34 relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child. The information shall be provided in writing, or by other means, including, where appropriate, by electronic means. When requested by the data subject, the information may be provided orally, provided that the identity of the data subject is proven by other means. | Article 8 of the PDPA: A government or non-government agency shall expressly inform the data subject of the following information when colleting their personal data in accordance with Article 15 or 19 of the PDPA: [...]<br><br>• the data subject's rights under Article 3 and the methods for exercising such rights; and<br>• the data subject's rights and interests that will be affected if he or she elects not to provide his or her personal data. |
| Article 12(1): The information shall be provided in writing, or by other means, including, where appropriate, by electronic means. When requested by the data subject, the information may be provided orally, provided that the identity of the data subject is proven by other means. | The PDPA and the Enforcement Rules do not contain any formal requirements as to the format of response. |
| Article 17(3): Paragraphs 1 and 2 shall not apply to the extent that processing is necessary:<br><br>(a) for exercising the right of freedom of expression and information;<br><br>(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;<br><br>(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);<br><br>(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<br><br>(e) for the establishment, exercise or defence of legal claims. | The PDPA and the Enforcement Rules do not explicitly provide any exceptions to this right. |





| GDPR | PDPA |
|---|---|
| **Differences (cont'd)** | |
| Article 12(5): Information provided under Articles 13 and 14 and any communication and any actions taken under Articles 15 to 22 and 34 shall be provided free of charge. Where requests from a data subject are manifestly unfounded or excessive, in particular because of their repetitive character, the controller may either:<br><br>(a) charge a reasonable fee taking into account the administrative costs of providing the information or communication or taking the action requested; or<br><br>(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**

The PDPA and GDPR require agencies and controllers, respectively, to provide information about processing activities to data subjects, irrespective of whether information is collected directly or indirectly from the data subject. Both pieces of legislation also establish the format through which personal information can be communicated and outline exemptions to this right. However, the GDPR requires more detailed disclosure than the PDPA, and addresses the intelligibility of information, whereas the PDPA does not.

| GDPR | PDPA |
|---|---|

## Similarities

Article 13(1): Where personal data relating to a data subject are collected from the data subject, the controller shall, at the time when personal data are obtained, provide the data subject with all of the following information:

(a) the identity and the 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; and

(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:

Article 8 of the PDPA: A government or non-government agency shall expressly inform the data subject of the following information when colleting their personal data in accordance with Article 15 or 19 of the PDPA:

- the name of the government or non-government agency;
- the purpose of the collection;
- the categories of the personal data to be collected;
- the time period, territory, recipients, and methods of which the personal data is used;
- the data subject's rights under Article 3 and the methods for exercising such rights; and
- the data subject's rights and interests that will be affected if he/she elects not to provide his/her personal data.





| GDPR | PDPA |
|---|---|

## Similarities (cont'd)

(a) the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;

(b) the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability;

(c) where the processing is based on point (a) of Article 6(1) or point (a) of Article 9(2), the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;

(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; and

(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.

Regarding the information to be provided see Article 13(1) and (2) above.

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

See Article 8 above.

Article 9 of the PDPA: A government or non-government agency shall, before processing or using the personal data collected in accordance with Article 15 or 19 which was not provided by the data subject, inform the data subject of its source of data and other information specified in Subparagraphs 1 to 5, Paragraph 1 of the preceding article. See Article 8 above.

The obligation to inform may be performed at the time of the first use of the personal data towards the data subject.

| GDPR | PDPA |
|---|---|

## Similarities (cont'd)

| GDPR | PDPA |
|---|---|
| See Article 12(1) above. | Article 16 of the Enforcement Rules: The obligation to inform data subjects as required under Articles 8, 9, and 54 of the PDPA may be fulfilled via verbal words, in writing, over the phone, via text messages, email, fax, electronic documents, or other means that can effectively make the information known or available to the data subjects. |
| The requirements of Article 13 do not apply where the data subject already has the information.<br><br>The requirements of Article 14 do not apply where:<br><br>(a) the data subject already has the information;<br><br>(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;<br><br>(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<br><br>(d) where the personal data must remain confidential subject to an obligation of professional secrecy regulated by Union or Member State law, including a statutory obligation of secrecy. | Article 8 of the PDPA: The obligation to inform as prescribed [...] may be waived under any of the following circumstances:<br><br>• where notification may be waived in accordance with the law;<br>• where the collection of personal data is necessary for the government agency to perform its statutory duties or the non-government agency to fulfil its statutory obligation;<br>• where giving notice will prevent the government agency from performing its statutory duties;<br>• where giving notice will harm public interests;<br>• where the data subject has already known the content of the notification; or<br>• where the collection of personal data is for non-profit purposes and clearly has no adverse effect on the data subject.<br><br>Article 9 of the PDPA: The obligation to inform [when not provided by the data subject] may be exempt under any of the following circumstances:<br><br>• under any of the circumstances provided in Paragraph 2 of the preceding article;<br>• where the personal data has been disclosed to the public by the data subject or has been made public lawfully;<br>• where it is unable to inform the data subject or his or her statutory representative;<br>• where it is necessary for statistics gathering or academic research in pursuit of public interests, provided that such data, as processed by the data provider or as disclosed by the data collector, may not lead to the identification of a specific data subject; or<br>• where the personal data is collected by mass communication enterprises for the purpose of news reporting for the benefit of public interests. |



| GDPR | PDPA |
|---|---|

## Differences

| GDPR | PDPA |
|---|---|
| Article 12(1): The controller shall take appropriate measures to provide any information referred to in Articles 13 and 14 and any communication under Articles 15 to 22 and 34 relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child. The information shall be provided in writing, or by other means, including, where appropriate, by electronic means. When requested by the data subject, the information may be provided orally, provided that the identity of the data subject is proven by other means. | The PDPA and the Enforcement Rules do not contain any intelligibility requirements in relation to the right to be informed. |

# 5.3. Right to object


The PDPA does not provide a general right to object, but does establish a specific right to object in relation to direct marketing as is the case in the GDPR. In addition, the PDPA provides data subjects with the right to demand the cessation of the collection, processing, or use of his or her personal data, and outlines requirements for the charging of fees and the responsibilities of agencies to notify data subjects of this right, similar to the GDPR. However, the PDPA does not address the withdrawal of consent or provide exemptions to this right.

| GDPR | PDPA |
|---|---|
| **Similarities** | |
| Article 21(1): The data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her which is based on point (e) or (f) of Article 6(1), including profiling based on those provisions. The controller shall no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims. | The PDPA does not provide for the right to object or opt/out of the processing of personal information.<br><br>However, Article 3(4) of the PDPA: A data subject shall be able to exercise the following rights with regard to his or her personal data and such rights shall not be waived or limited contractually in advance [...] the right to demand the cessation of the collection, processing or use of his or her personal data.<br><br>Article 11 of the PDPA: In the event of a dispute regarding the accuracy of the personal data, the government or non-government agency shall, on its own initiative or upon the request of the data subject, cease processing or using the personal data, unless the processing or use is either necessary for the performance of an official or business duty, or has been agreed to by the data subject in writing, and the dispute has been recorded.<br><br>In addition, when the specific purpose of data collection no longer exists, or upon expiration of the relevant time period, the government or non-government agency shall, on its own initiative or upon the request of the data subject,<br><br>erase or cease processing or using the personal data, unless the processing or use is either necessary for the performance of an official or business duty, has been agreed to by the data subject in writing, [...] and erase personal data collected or cease collecting, processing, or using the personal data in the event where the collection, processing or use of the personal data is in violation of the PDPA. |





| GDPR | PDPA |
|---|---|
| **Similarities (cont'd)** | |
| Article 21(3): Where the data subject objects to processing for direct marketing purposes, the personal data shall no longer be processed for such purposes. | Article 20 of the PDPA: When a non-government agency uses personal data for marketing purpose pursuant to the preceding paragraph, upon the data subject's objection to such use, the agency shall cease using the data subject's personal data for marketing.<br><br>A non-government agency, when using the data subject's personal data for marketing purpose for the first time, shall provide the data subject of the ways that he or she can object to such use, and the agency shall pay for the fees therefrom. |
| 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. | Article 8 of the PDPA: A government or non-government agency shall expressly inform the data subject of the following information when colleting their personal data in accordance with Article 15 or 19 of the PDPA: [...]<br><br>the data subject's rights under Article 3 and the methods for exercising such rights; and<br>the data subject's rights and interests that will be affected if he or she elects not to provide his or her personal data. |
| Regarding feees see Article 12(5) in section 5.1. above. | See Article 14 of the PDPA in section 5.1. above. |
| Regarding the response timeframe see Article 12(3) in section 5.1. above. | See Article 13 PDPA in section 5.1. above. |

| GDPR | PDPA |
|---|---|
| **Differences** | |
| Article 7(3): The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw as to give consent. | The PDPA and the Enforcement Rules do not directly address the withdrawal of consent. |
| Article 18(1): The data subject shall have the right to obtain from the controller restriction of processing where one of the following applies:<br><br>(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;<br><br>(b) the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead;<br><br>(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; or<br><br>(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. | The PDPA and the Enforcement Rules do not provide for the right to restrict processing. |
| See Article 12(1) in section 5.1. above. | The PDPA and the Enforcement Rules do not contain any formal requirements as to the format of response. |
| See Article 12(5) in section 5.1. above. | The PDPA and the Enforcement Rules do not directly provide exceptions to this right. |






## 5.4. Right of access

The PDPA establishes a right to inquire and review personal data being processed by an agency. However, while the GDPR details specific information which is able to be accessed, and outlines verification requirements, the PDPA does not provide such information. Nonetheless, the PDPA does provide requirements for the charging of fees, the responsibilities of agencies to notify data subjects of this right, response times, and exceptions to this right.

| GDPR | PDPA |
|---|---|
| **Similarities** | |
| 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. | Article 3(1) of the PDPA: A data subject shall be able to exercise the following rights with regard to his or her personal data and such rights shall not be waived or limited contractually in advance [...] the right to make an inquiry of and to review his or her personal data. |
| Regarding the requirement to inform the data subject of the right, s ee Article 12(1) in section 5.1. | See Article 8 of the PDPA in section 5.1. above. |
| Regarding the fees, see Article 12(5) in section 5.1. above. | See Article 14 of the PDPA in section 5.1. above. |
| See Article 12(3) in section 6.1. above. | Article 13 of the PDPA: where a request is made by a data subject to a government or non-government agency pursuant to Article 10, the agency shall determine whether to accept or reject such request within 15 days; such deadline may be extended by up to 15 days if necessary, and the data subject shall be notified in writing of the reason for the extension. |
| See Article 12(5) in section 6.1. above. | Article 10 of the PDPA: Upon the request of a data subject, the government or non-government agency shall reply to the data subject's inquiry, allow the data subject to review the personal data collected, or provide the data subject with a copy thereof except under any of the following circumstances:<br><br>where national security, diplomatic or military secrets, overall economic interests or other material national interests may be harmed;<br>where a government agency may be prevented from performing its statutory duties; or<br>where the material interests of the data collectors or any third parties may be adversely affected. |

| GDPR | PDPA |
|---|---|
| **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:<br><br>(a) the purposes of the processing;<br><br>(b) the categories of personal data concerned;<br><br>(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;<br><br>(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;<br><br>(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;<br><br>(f) the right to lodge a complaint with a supervisory authority;<br><br>(g) where the personal data are not collected from the data subject, any available information as to their source; and<br><br>(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. | The PDPA and the Enforcement Rules do not directly outline the information to be accessed. |
| Recital 64: The controller should use all reasonable measures to verify the identity of a data subject who requests access, in particular in the context of online services and online identifiers. A controller should not retain personal data for the sole purpose of being able to react to potential requests. | The PDPA and the Enforcement Rules do not explicitly refer to identity verification requirements. |
| See Article 12(1) in section 5.1. above. | The PDPA and the Enforcement Rules do not contain any formal requirements as to the format of response. |





## 5.5. Right not to be subject to discrimination


The PDPA and the GDPR do not specifically refer to the right not to be subject to discrimination. In addition, unlike the GDPR, the PDPA does not provide a right not to be subjected to decisions based solely on automated processing.

| GDPR | PDPA |
|---|---|
| **Differences** | |
| The GDPR only implies this right and does not provide an explicit definition for it. | The PDPA and the Enforcement Rules do not refer to this right. |
| Article 22(1): The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her. [Article 22 goes on to detail this right, including exceptions] | The PDPA and the Enforcement Rules do not refer to automated processing. |

## 5.6. Right to data portability

Inconsistent

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

| GDPR | PDPA |
|---|---|

### Differences

| GDPR | PDPA |
|---|---|
| Article 20(1) of the GDPR: The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided, where:<br><br>(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<br><br>(b) the processing is carried out by automated means. | The PDPA and the Enforcement Rules do not explicitly refer to a right to data portability. |
| See Article 12(1) in section 5.1. | The PDPA and the Enforcement Rules do not explicitly refer to a right to data portability. |
| See Article 12(5) in section 5.1. above. | The PDPA and the Enforcement Rules do not explicitly refer to a right to data portability. |
| See Article 12(3) in section 5.1. above. | The PDPA and the Enforcement Rules do not explicitly refer to a right to data portability. |
| See Article 20(1) above. | The PDPA and the Enforcement Rules do not explicitly refer to a right to data portability. |
| Article 20(2): In exercising his or her right to data portability pursuant to paragraph 1, the data subject shall have the right to have the personal data transmitted directly from one controller to another, where technically feasible. | The PDPA and the Enforcement Rules do not explicitly refer to a right to data portability. |
| See Article 20(2) above. | The PDPA and the Enforcement Rules do not explicitly refer to a right to data portability. |
| See Article 12(5) in section 5.1. above. | The PDPA and the Enforcement Rules do not explicitly refer to a right to data portability. |





# 6. Enforcement

Fairly inconsistent

## 6.1. Monetary penalties

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

| GDPR | PDPA |
|---|---|

### Similarities

| GDPR | PDPA |
|---|---|
| The GDPR provides for monetary penalties. | The PDPA provides for monetary penalties. |

### Differences

| GDPR | PDPA |
|---|---|
| Article 58(2) Each supervisory authority shall have all of the following corrective powers:<br><br>[...] (i): to impose an administrative fine pursuant to Article 83, in addition to, or instead of measures referred to in this paragraph, depending on the circumstances of each individual case. | Article 25 of the PDPA: In the event that a non-government agency has violated the PDPA, the central government authority in charge of the industry concerned or the municipality/city/county government concerned may impose fines on the non-government agency in accordance with the PDPA. |
| Article 83(5): infringements of the following provisions shall, in accordance with paragraph 2, be subject to administrative fines up to €20 million, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher:<br><br>(a) the basic principles for processing, including conditions for consent, pursuant to Articles 5, 6, 7 and 9;<br><br>(b) the data subjects' rights pursuant to Articles 12 to 22;<br><br>(c) the transfers of personal data to a recipient in a third country or an international organisation pursuant to Articles 44 to 49;<br><br>(d) any obligations pursuant to Member State law adopted under Chapter IX; or<br><br>(e) non-compliance with an order or a temporary or definitive limitation on processing or the suspension of data flows by the supervisory authority pursuant to Article 58(2) or failure to provide access in violation of Article 58(1). | Article 41 of the PDPA: If a person, with the intention of obtaining unlawful gains for himself/herself or a third party, or with the intention of impairing another person's interests, is in violation of Paragraph 1, Article 6, Articles 15, 16, 19, and Paragraph 1, Article 20, or an order or decision relating to the restrictions on cross-border transfers made by the central government authority in charge of the industry concerned in accordance with Article 21 of the PDPA, thereby causing damage to others the person shall be sentenced to imprisonment for no more than five years; in addition thereto, a fine of no more than TWD 1 million (approx. €31,770) may be imposed.<br><br>Article 42 of the PDPA: If a person, with the intention of obtaining unlawful gains for himself or herself or for a third party, or infringing upon the interests of others, illegally changes or erases personal data files, or otherwise compromises the accuracy of another's personal data files, thereby causing damages to others, the person shall be sentenced to imprisonment for no more than five years or detention, and/or a fine of no more than TWD 1 million (approx. €31,770). |

| GDPR | PDPA |
|---|---|

## Differences (cont'd)

| | |
|---|---|
| (6) Non-compliance with an order by the supervisory authority as referred to in Article 58(2) shall, in accordance with paragraph 2 of this Article, be subject to administrative fines up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher. | Article 44 of the PDPA: A government official who abuses the power, opportunity or means available to him/her to commit any of the offenses described in this Chapter shall be subject to a more severe punishment which is up to 50% more than that prescribed above. |
| Under Article 83(4), (5), and (6), fines may be issued that equate to 2% or 4% of the total worldwide annual turnover of the preceding financial year. | The PDPA and the Enforcement Rules do not provide monetary penalties in the form of percentage of turnover. |
| Article 83(2): When deciding whether to impose an administrative fine and deciding on the amount of the administrative fine in each individual case due regard shall be given to the following:<br><br>(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;<br><br>(b) the intentional or negligent character of the infringement;<br><br>(c) any action taken by the controller or processor to mitigate the damage suffered by data subjects;<br><br>(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;<br><br>(e) any relevant previous infringements by the controller or processor;<br><br>(f) the degree of cooperation with the supervisory authority, in order to remedy the infringement and mitigate the possible adverse effects of the infringement;<br><br>(g) the categories of personal data affected by the infringement;<br><br>(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; | The PDPA does not expressly refer to mitigating factors. |





GDPR | PDPA

Differences (cont'd)

| | |
|---|---|
| (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;<br><br>(j) adherence to approved codes of conduct pursuant to Article 40 or approved certification mechanisms pursuant to Article 42; and<br><br>(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. | |
| Imprisonment is not applicable under the GDPR. | See Articles 41 and 42 of the PDPA outlined above. |

# 6.2. Supervisory authority


The PDPA provides oversight powers to the Ministry of justice as well as central government authorities (the powers of the Ministry of Justice have been transferred to the NDC). Similar to the GDPR, central government authorities have investigatory, corrective, and advisory powers. However, unlike the GDPR which details the tasks of the data protection authorities, the PDPA does not provide detailed information on this matter, nor does it require the submission of an annual report by central government authorities.

| GDPR | PDPA |
|---|---|

## 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').

The PDPA does not explicitly provide for the appointment of a data protection authority. However, Article 53 of the PDPA provides that the Ministry of Justice shall, in conjunction with the central government authorities in charge of the industries concerned, set forth the specific purposes and categories of personal data, and provide the same to government and non-government agencies for reference and use (the powers of the Ministry of Justice have been transferred to the NDC).

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.

Article 22 of the PDPA: The central government authorities in charge of the industries concerned or the municipality/city/county governments concerned may, when they deem necessary or suspect any possible violation of the PDPA, inspect compliance with the security control measures, the guidelines on disposing personal data upon business termination, and the restrictions on cross-border transfers, or conduct any other routine inspections by having their staff enter non-government agencies' premises upon presentation of their official identification documents and order relevant personnel at the non-government agencies to provide necessary explanations, cooperate on adopting relevant measures, or provide supporting documents.





| GDPR | PDPA |
|---|---|

## Similarities (cont'd)

Article 58(2): Each supervisory authority shall have all of the following corrective powers:

(a) to issue warnings to a controller or processor that intended processing operations are likely to infringe provisions of this Regulation;

(b) to issue reprimands to a controller or a processor where processing operations have infringed provisions of this Regulation;

(c) to order the controller or the processor to comply with the data subject's requests to exercise his or her rights pursuant to this Regulation;

(d) to order the controller or processor to bring processing operations into compliance with the provisions of this Regulation, where appropriate, in a specified manner and within a specified period;

(e) to order the controller to communicate a personal data breach to the data subject;

(f) to impose a temporary or definitive limitation including a ban on processing;

(g) to order the rectification or erasure of personal data or restriction of processing pursuant to Articles 16, 17 and 18 and the notification of such actions to recipients to whom the personal data have been disclosed pursuant to Article 17(2) and Article 19;

(h) to withdraw a certification or to order the certification body to withdraw a certification issued pursuant to Articles 42 and 43, or to order the certification body not to issue certification if the requirements for the certification are not or are no longer met;

(i) to impose an administrative fine pursuant to Article 83, in addition to, or instead of measures referred to in this paragraph, depending on the circumstances of each individual case; and

(j) to order the suspension of data flows to a recipient in a third country or to an international organisation.

Article 25 of the PDPA: In the event that a non-government agency has violated the PDPA, the central government authority in charge of the industry concerned or the municipality/city/county government concerned may [...] enforce the following corrective measures:

- prohibit the collection, processing or use of the personal data;
- order the erasure of the processed personal data and personal data files;
- confiscate or order the destruction of the unlawfully collected personal data; and/or
- disclose to the public the violation of the non-government agency, the name of the non-government agency and its responsible person/representative.

In addition, where the central government authority in charge of the industry concerned or the municipality/city/county government concerned enforce the corrective measures referred to above, such measures shall be within the scope that is necessary to prevent and remedy the violation of the PDPA and shall do the least harm to the rights and interests of the non-government agency concerned.

| GDPR | PDPA |
|---|---|

## Similarities (cont'd)

| GDPR | PDPA |
|---|---|
| Article 58(3): Each supervisory authority shall have all of the following authorisation and advisory powers:<br><br>(a) to advise the controller in accordance with the prior consultation procedure referred to in Article 36;<br><br>(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;<br><br>(c) to authorise processing referred to in Article 36(5), if the law of the Member State requires such prior authorisation;<br><br>(d) to issue an opinion and approve draft codes of conduct pursuant to Article 40(5);<br><br>(e) to accredit certification bodies pursuant to Article 43;<br><br>(f) to issue certifications and approve criteria of certification in accordance with Article 42(5);<br><br>(g) to adopt standard data protection clauses referred to in Article 28(8) and in point (d) of Article 46(2);<br><br>(h) to authorise contractual clauses referred to in point (a) of Article 46(3);<br><br>(i) to authorise administrative arrangements referred to in point (b) of Article 46(3); and<br><br>(j) to approve binding corporate rules pursuant to Article 47. | Article 27 of the PDPA: The central government authorities in charge of the industries concerned may designate and order certain non-government agencies to establish a security and maintenance plan for the protection of personal data files and a guideline on disposing personal data following a business termination. Matters such as standards on setting forth the aforementioned plans and disposal regulations shall be expressly established by the central government authority of in charge of the industry concerned. |



| GDPR | PDPA |
|---|---|

## Differences

| GDPR | PDPA |
|---|---|
| Article 57(1): Without prejudice to other tasks set out under this Regulation, each supervisory authority shall on its territory:<br><br>(a) monitor and enforce the application of this Regulation;<br><br>(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;<br><br>(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;<br><br>(d) promote the awareness of controllers and processors of their obligations under this Regulation;<br><br>(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;<br><br>(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;<br><br>(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;<br><br>(h) conduct investigations on the application of this Regulation, including on the basis of information received from another supervisory authority or other public authority;<br><br>(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; | The PDPA and the Enforcement Rules do not explicitly outline the duties of central government authorities in a comprehensive manner.<br><br>Article 53 of the PDPA: The Ministry of Justice shall, in conjunction with the central government authorities in charge of the industries concerned, set forth the specific purposes and categories of personal data, and provide the same to government and non-government agencies for reference and use. |

| GDPR | PDPA |
|---|---|

## Differences (cont'd)

(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;

(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.





| GDPR | PDPA |
|---|---|

## Differences (cont'd)

| GDPR | PDPA |
|---|---|
| Article 59: Each supervisory authority shall draw up an annual report on its activities, which may include a list of types of infringement notified and types of measures taken in accordance with Article 58(2). Those reports shall be transmitted to the national parliament, the government and other authorities as designated by Member State law. They shall be made available to the public, to the Commission and to the Board. | The PDPA and the Enforcement Rules do not explicitly require to draw up an annual report. |

# 6.3. Civil remedies for individuals

**Fairly inconsistent**

The PDPA and the GDPR both provide data subjects with a right to claim, as well as a right to receive compensation for damage suffered as a result of non-compliance. However, the PDPA does not address matters such as data subject representation, the liability of processors, and outlines specific compensation amounts for data subjects.

| GDPR | PDPA |
|---|---|

## Similarities

| GDPR | PDPA |
|---|---|
| Article 79: Without prejudice to any available administrative or non-judicial remedy, including the right to lodge a complaint with a supervisory authority pursuant to Article 77, each data subject shall have the right to an effective judicial remedy where he or she considers that his or her rights under this Regulation have been infringed as a result of the processing of his or her personal data in non-compliance with this Regulation. | Article 28 of the PDPA: If an injury suffered by the victim is a non-pecuniary damage, he or she may request an appropriate amount of monetary compensation; if the injury suffered by the victim is damage to his or her reputation, the victim may request appropriate corrective measures to restore his or her reputation.<br><br>The right of claim referred to in Paragraph 2 above may not be transferred or inherited. However, this does not apply to the circumstances where monetary compensation has been agreed upon in a contract or a claim therefor has been filed with the court. |
| 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. | See Article 28 of the PDPA outlined above. |

## Differences

| GDPR | PDPA |
|---|---|
| Article 80(1): The data subject shall have the right to mandate a not-for-profit body, organisation or association which has been properly constituted in accordance with the law of a Member State, has statutory objectives which are in the public interest, and is active in the field of the protection of data subjects' rights and freedoms with regard to the protection of their personal data to lodge the complaint on his or her behalf, to exercise the rights referred to in Articles 77, 78 and 79 on his or her behalf, and to exercise the right to receive compensation referred to in Article 82 on his or her behalf where provided for by Member State law. | The PDPA and the Enforcement Rules do not explicitly address the right to mandate representation. |
| Not applicable. | Article 28 of the PDPA: Under the circumstances outlined above, it is difficult or impossible for the victim to prove the monetary value of the actual damage, he or she may ask the court to award the compensation in the amount of at least TWD 500 (approx. €16) but no more than TWD 20,000 (approx. €630) per incident, per person based on the severity of the damage.<br><br>Where the rights of multiple data subjects have been infringed upon due to the same incident, the total amount of compensation awarded to such data subjects shall not exceed TWD 200 million (approx. € 6.36 million). However, if the interests involved in the incident exceed TWD 200 million (approx. € 6.36 million), the compensation shall be up to the value of such interests.<br><br>If the total amount of damages for the injuries attributable to the same incident exceeds the amount referred to in the preceding paragraph, the compensation payable to each victim shall not be limited to the lower end of damages, i.e. TWD 500 (approx. €16), per incident as set forth in Paragraph 3 of this Article. |
| Article 82(2): Any controller involved in processing shall be liable for the damage caused by processing which infringes this Regulation. A processor shall be liable for the damage caused by processing only where it has not complied with obligations of this Regulation specifically directed to processors or where it has acted outside or contrary to lawful instructions of the controller. | The PDPA does not explicitly address the liability of entities acting on behalf of the commissioning agency. |
| Article 82(3): A controller or processor shall be exempt from liability under paragraph 2 if it proves that it is not in any way responsible for the event giving rise to the damage. | Article 29 of the PDPA: A non-government agency shall be liable for the damages arising from any injury caused by any unlawful collection, processing or use of personal data, or other infringement on the rights of data subjects due to such non-government agency's violation of the PDPA, unless the non-government agency can prove that such injury is not caused by its wilful act or negligence.<br><br>Article 30 of the PDPA: The right to claim damage compensation will be extinguished if the right-holder does not exercise such right within the two-year period after he or she becomes aware of his or her damage and the identity of the person(s) liable for the compensation, or the five-year period following the occurrence of the damage. |