

Singapore - Third Country Assessment

September 2025

1. Applicable Law

1.1. Rules of law, human rights, and data protection/privacy regime

Is the principle of the rule of law provided in the legal system?

The principle of the rule of law in Singapore is recognized and provided for in Singapore's legal system, notably through the separation of Governmental powers among the three branches of the [Government of the Republic of Singapore](#) (the Government), namely the Executive, the Legislature, and the Judiciary. The checks and balances amongst the different branches of the Government are embedded in the [Constitution of the Republic of Singapore](#) (the Constitution) as follows:

- the executive authority is vested in the [President of the Republic of Singapore](#) (the President) and their cabinet (Article 23 of the Constitution);
- the legislative power of Singapore is vested in the Legislature, which consists of the President and the [Parliament of Singapore](#) (the Parliament)(Article 38 of the Constitution); and
- the judicial power is vested in the [Supreme Court of Singapore](#) and in such subordinate courts as may be provided for by written law (Article 93 of the Constitution).

Are there laws which protect human rights and fundamental freedoms?

Part IV of the Constitution protects fundamental liberties, such as the right to life and personal liberty, equal protection of the law, the freedom of speech, assembly, and association, and the freedom of religion.

In addition, there is a broad framework of common law and statutory torts in Singapore, which indirectly protect privacy-related interests (e.g., nuisance, trespass to the person, defamation, and law of confidence). Moreover, the [Protection from Harassment Act 2014 \(2020 Revised Edition\)](#) enshrines, in statute, the tort of harassment and provides a range of remedies against harassment and false statements of fact.

Is there a comprehensive data protection/privacy law?

The primary data protection legislation in Singapore is the [Personal Data Protection Act 2012 \(No. 26 of 2012\)](#) (PDPA), which sets out a baseline standard of protection for personal data across organizations. The PDPA operates concurrently with sector-specific laws and regulations, which may also address the issues relating to privacy and data protection.

Are there sectoral data protection/privacy laws?

Some sectoral data protection regulations that impose additional data protection requirements in relation to regulated entities include:

- the [Healthcare Services Act 2020 \(No. 3 of 2020\)](#), which addresses the confidentiality of medical information and the retention of medical records;
- the [Code of Practice for Competition in the Provision of Telecommunications and Media Services 2022](#), issued under the [Info-communications Media Development Authority Act 2016](#) and [Telecommunications Act 1999 \(2020 Revised Edition\)](#) (TA), which governs the use of end-user service information by telecoms licensees and other specified persons; and
- the [Banking Act 1970 \(2020 Revised Edition\)](#) (the Banking Act) contains banking secrecy provisions, which govern customer information obtained by banks.

The above legislations are administered and enforced by the relevant sector regulators, namely the [Ministry of Health](#) (MOH), the [Infocomm Media Development Authority](#) (IMDA), and the [Monetary Authority of Singapore](#) (MAS), respectively.

Is there relevant case law regarding privacy and/or data protection?

Since 2016, the [Personal Data Protection Commission](#) (PDPC), which is in charge of administering and enforcing the PDPA, has published enforcement decisions that are helpful in clarifying the requirements under the PDPA. These enforcement decisions are generally accessible via the PDPC's [website](#).

As of August 2025, the PDPC has published a total of 260 grounds of decisions or summaries of grounds of decisions, with a significant majority of these cases relating to breaches of the 'protection obligation' (Section 24 of the PDPA) due to inadequate security measures being taken to safeguard the personal data of the individuals.

Apart from the decisions published by the PDPC, there are cases in which the PDPA has been considered by the Singapore courts. In September 2022, the Singapore Court of Appeal (Court of Appeal) handed down its decision in the case of [Michael Reed v. Alex Bellingham and Attorney-General, intervener](#) ([2022] SGCA 60), wherein it held that emotional distress could constitute 'loss or damage', such that private action could be brought under Section 48O(1) of the PDPA. This decision reverses the Singapore High Court's earlier decision, in the case [Alex Bellingham v. Michael Reed](#) ([2021] SGHC 125), on the same matter in 2021. The Court of Appeal also held that the loss of control of personal data is not actionable.

What are the legitimate legal bases for processing personal data in a lawful, fair, and legitimate way?

Generally, the processing of personal data is expressed in terms of 'collection, use, and disclosure' of the same under the PDPA. An organization is required to obtain the consent of an individual before collecting, using, or disclosing their personal data for a purpose (the consent obligation), unless otherwise required or authorized by law (Section 13 of the PDPA).

Pursuant to Section 14 of the PDPA, consent is only validly obtained if the individual has been informed of the purposes for the collection, use, or disclosure of the personal data on or before the collection of the personal data, and the individual has provided consent for that purpose in accordance with the PDPA (please refer to the section on requirements to inform individuals in relation to processing activities below). The purposes must also be what a reasonable person would consider appropriate in the circumstances. Fresh consent must be obtained where the

personal data collected is to be used for a new purpose, i.e., different from the purpose that the individual originally consented to.

In addition, organizations should note that consent is not considered as validly obtained in the following scenarios:

- where consent is obtained as a condition of providing a product or service, and such consent is beyond what is reasonable to provide the product or service to the individual; and
- where false or misleading information is provided, or deceptive or misleading practices are used, in order to obtain or attempt to obtain consent.

Sections 15 and 15A of the PDPA also provide for different forms of deemed consent, namely:

- deemed consent by conduct;
- deemed consent by contractual necessity; and
- deemed consent by notification.

Deemed consent by conduct applies to situations where the individual has voluntarily provided their personal data to the organization, for purposes that are objectively obvious and reasonably appropriate from the surrounding circumstances.

Deemed consent by contractual necessity is where individuals have provided their personal data to one organization for the purpose of a transaction, and it is reasonably necessary for the organization to disclose the personal data to a second organization for the conclusion or performance of a contract or transaction between the individual and the first organization. Deemed consent by contractual necessity also allows for the second organization to further disclose the personal data to subsequent organizations downstream, where the use or disclosure is reasonably necessary to conclude or perform the contract between the individual and the first organization (among others).

Under deemed consent by notification, an individual may be deemed to have consented to the collection, use, or disclosure of personal data for a purpose that the individual had been notified of, and where that individual has not taken any action to opt out of the collection, use, or disclosure of their personal data. For an organization to rely on deemed consent by notification, the organization must:

- conduct an assessment to determine that the proposed collection, use, or disclosure of personal data is not likely to have an adverse effect on the individual. This includes identifying and implementing reasonable measures to eliminate, mitigate, or reduce the likelihood that any such adverse effect will occur;
- take reasonable steps to notify the individual of the organization's intention to collect, use, or disclose the personal data and the purpose of such collection, use, or disclosure; and
- provide a reasonable period for the individual to opt out before the organization proceeds to collect, use, or disclose the personal data.

Consent for the collection, use, or disclosure of personal data is deemed to be given only after the opt-out period has lapsed. Further, an individual can withdraw consent for the collection,

use, or disclosure of personal data after the opt-out period has lapsed if the individual no longer wishes to consent to the purpose.

1.2. Data protection principles

Is the purpose limitation principle provided by the data protection/ privacy law?

Yes, Section 18 of the PDPA provides that an organization may only collect, use, or disclose personal data for purposes that a reasonable person would consider appropriate in the circumstances (the purpose limitation obligation), and where applicable, that the individual has been informed of by the organization (please see the section on requirements to inform individuals in relation to processing activities below).

Is the accuracy principle provided by the data protection/privacy law?

Yes, Section 23 of the PDPA provides that an organization must make a reasonable effort to ensure that personal data collected is accurate and complete if it is likely to use such personal data to make a decision that affects the individual concerned or to disclose such personal data to another organization (the accuracy obligation).

Does the law provide for the processing to be adequate, relevant, and not excessive?

While the PDPA does not expressly provide for a data minimization principle, the purpose limitation obligation (please refer to the section on the purpose limitation principle above) and the retention limitation obligation (please refer to the section on keeping personal data longer than necessary below) operate to limit the collection, use, disclosure, and retention of personal data by organizations.

Does the law provide that personal data must not be kept for longer than necessary?

Yes, Section 25 of the PDPA provides that an organization must cease to retain documents containing personal data or remove the means by which the personal data can be associated with particular individuals, as soon as it is reasonable to assume that the retention of such personal data no longer serves the purpose for which it was collected and it is no longer necessary for legal or business purposes (the retention limitation obligation).

Does the law require that data is to be processed in a secure way?

Yes, Section 24 of the PDPA provides that an organization must protect personal data in its possession or under its control by making reasonable security arrangements to prevent (the protection obligation):

- the unauthorized access, collection, use, disclosure, copying, modification, disposal, or similar risks; and
- the loss of any storage medium or device on which personal data is stored.

Does the law require data controllers to inform individuals in relation to the processing activity?

Section 20 of the PDPA provides that an organization must notify an individual of the purpose(s) for which it intends to collect, use, or disclose his or her personal data, on or before such collection, use, or disclosure (the notification obligation). While the PDPA does not specify a particular manner or form in which an organization is to inform an individual of the purposes,

the PDPC has stated in its [Advisory Guidelines on Key Concepts in the PDPA](#) (revised May 16, 2022) (the Advisory Guidelines), that organizations should ensure that their notifications are clear, easily comprehensible, and easily accessible.

1.3. Individuals' rights

Does the law provide individuals with the right to obtain confirmation of processing and a right to access their data?

Section 21 of the PDPA provides for an individual's right to request an organization to provide access to the individual's personal data.

Unless an exception applies, an organization is required to, on request by an individual, provide them with (the access obligation):

- their personal data that is in the possession or under the control of the organization; and
- information about the ways in which that personal data has been or may have been used or disclosed by the organization within a year before the date of the individual's request.

Pursuant to Section 21(3) of the PDPA, organizations are prohibited from providing an individual with their personal data or other information if the provision of that personal data or other information could reasonably be expected to:

- threaten the safety or physical or mental health of an individual other than the individual who made the request;
- cause immediate or grave harm to the safety or to the physical or mental health of the individual who made the request;
- reveal personal data about another individual;
- reveal the identity of an individual who has provided personal data about another individual, and the individual providing the personal data does not consent to the disclosure of their identity; or
- be contrary to the national interest.

However, the exceptions mentioned in bullet points 3 and 4 above do not apply to any user activity data or any user-provided data from the individual who made the request, even if such data contains personal data about another individual.

In addition, the Fifth Schedule to the PDPA also sets out other exceptions to the access obligation, where organizations are not required to provide the information to individuals upon request. These include, but are not limited to:

- opinion data kept solely for an evaluative purpose;
- personal data which, if disclosed, would reveal confidential commercial information that could, in the opinion of a reasonable person, harm the competitive position of the organization; and

- personal data collected, used, or disclosed without consent, for the purposes of an investigation if the investigation and associated proceedings and appeals have not been completed.

Does the law empower individuals with a right to obtain rectification of their personal data?

Section 22 of the PDPA provides that an individual has the right to request that an organization correct an error or omission in their personal data (the correction obligation).

An organization is required to, on request by an individual:

- correct an error or omission in the individual's personal data that is in the possession or under the control of the organization; and
- send the corrected personal data to every other organization to which the personal data was disclosed by the organization within a year before the date of the correction request unless that other organization does not need the corrected personal data for any legal or business purpose.

However, an organization is not required to comply with the correction obligation in respect of the matters specified in the Sixth Schedule to the PDPA. These include, but are not limited to:

- opinion data kept solely for an evaluative purpose;
- a document related to a prosecution if proceedings related to the prosecution have not been completed; and
- derived personal data.

Does the law empower individuals with a right to obtain erasure of their personal data?

Although an individual may withdraw consent for the collection, use, or disclosure of his personal data by an organization, the PDPA does not require an organization to delete or destroy the individual's personal data upon request. Organizations may retain personal data in accordance with the data protection provisions under the PDPA.

Does the law empower individuals with a right to object to processing in specific circumstances?

Although an individual may withdraw consent for the collection, use, or disclosure of his personal data by an organization, there is no separate right to object. Organizations can process personal data if there is an applicable exception to consent under the PDPA. Under such circumstances, individuals may not have the right to object to the processing of their personal data insofar as the collection, use, or disclosure of their personal data without consent is authorized under the PDPA.

For example, there is an exception under the PDPA that allows organizations to collect, use, or disclose personal data of individuals without their consent where such collection, use, or disclosure of personal data is in the legitimate interests of the organization or another person, and the legitimate interests of the organization or other person outweighs any adverse effect on the individual (Part 3 of the First Schedule to the PDPA).

However, in order for an organization to rely on the legitimate interests exception, the organization must conduct an assessment to determine whether the criteria for relying on the exception are met, and provide the individual with reasonable access to information about the organization's collection, use, or disclosure of personal data. Therefore, organizations that rely on the legitimate interests exception to collect, use, or disclose personal data must make it known to individuals that they are relying on this exception to collect, use, and disclose personal data without consent.

If an individual is of the view that an organization has failed to comply with the requirements under the PDPA (such as the conditions for relying on the legitimate interests exception), they may submit a complaint to the PDPC (please refer to the section on legal remedies for data subjects below).

Does the law provide a right to object to processing for direct marketing at any time and without any charge?

Organizations must obtain express consent from individuals for the purpose of sending direct marketing messages. In particular, organizations are not permitted to rely on the legitimate interests exception or deemed consent by notification for the purpose of sending direct marketing messages.

Pursuant to Section 16 of the PDPA, an individual may, at any time upon giving reasonable notice to an organization, withdraw the consent given (including consent deemed to have been given under the PDPA) for the collection, use, or disclosure of their personal data by the organization for any purpose.

On receipt of the individual's notice, the organization must inform the individual of the likely consequences of withdrawal. The organization must not prohibit an individual from withdrawing consent, although this does not affect any legal consequences arising from such withdrawal.

Upon withdrawal of consent, the organization must cease, and cause its data intermediaries and agents to cease, collecting, using, or disclosing the personal data unless the collection, use, or disclosure of personal data without consent is otherwise authorized under the PDPA or any other written law.

In addition, organizations that wish to send direct marketing messages to Singapore telephone numbers via voice call, text, or fax must comply with the 'Do Not Call' provisions as set out in Parts 9 and 9A of the PDPA. Amongst other matters, the Do Not Call provisions establish separate Do Not Call registers for telephone calls, text messages, and faxes, and individuals who do not wish to receive marketing messages may register on one or more of these registers depending on their preference.

Does the law address when decisions based solely on automated processing (including profiling) may take place?

The PDPA does not currently address or differentiate between automated or non-automated processing of personal data by organizations.

Does the data protection system provide for limitations to the exercise of individuals' rights?

The PDPA provides a number of exceptions to various data protection obligations that organizations are required to comply with, in order to address situations where organizations

may have a legitimate need, for example, to collect, use, or disclose personal data without the individual's consent or to refuse to provide an individual with access to his personal data (please refer to our responses to the section on individuals' rights above).

However, Section 4(6)(a) of the PDPA provides that the data protection provisions do not affect any authority, right, privilege, or immunity conferred, or obligation or limitation imposed, by or under the law, except that performance of a contractual obligation shall not be an excuse for contravening the PDPA. This means that organizations are required to comply with their other legal obligations, for example, to protect confidential information.

Organizations should also note Section 4(6)(b) of the PDPA, which provides that the provisions of other written laws will prevail over the data protection provisions to the extent that any data protection provision is inconsistent with the provisions of the other written laws.

Does the law provide for specific protections for special categories of personal data?

The PDPA currently does not expressly differentiate or distinguish between special categories of personal data to which specific protections should apply.

However, organizations may have to implement more stringent measures in respect of sensitive data to comply with the PDPA. In particular, organizations should note that in relation to the requirement to make 'reasonable security arrangements' pursuant to the Protection Obligation under Section 24 of the PDPA (please refer to the section on requirements to inform individuals in relation to their processing activity above), the PDPC has stated in the Advisory Guidelines that each organization should consider adopting security arrangements that are reasonable and appropriate in the circumstances, for example, taking into consideration the nature of the personal data, the form in which the personal data has been collected, and the possible impact to the individual concerned if an unauthorized person obtained, modified, or disposed of the personal data.

1.4. Onward transfers

Does the law include rules for onward data transfers to third countries or international organizations?

Section 26 of the PDPA states that an organization must not transfer personal data to a country or territory outside Singapore except in accordance with the requirements prescribed under the PDPA to ensure that organizations provide a standard of protection to the personal data that is comparable to the protection under the PDPA (the transfer limitation obligation).

Under Regulation 10 of the [Personal Data Protection Regulations 2021](#) (PDPR), the transferring organization must, before transferring the personal data to a country or territory outside of Singapore, take appropriate steps to ascertain whether and to ensure that, the recipient is bound by legally enforceable obligations to provide the personal data transferred with a standard of protection comparable to the protection under the PDPA.

'Legally enforceable obligations' is defined in Regulation 11 of the PDPR to include obligations imposed on the recipient under:

- any law;
- any contract that requires the recipient to provide to the transferred personal data a standard of protection that is at least comparable to the protection under the PDPA, and

which specifies the countries and territories to which the personal data may be transferred under the contract;

- any Binding Corporate Rules (BCRs) (in cases where a recipient is an organization related to the transferring organization) that require every recipient to provide to the transferred personal data a standard of protection that is at least comparable to the protection under the PDPA, and which specifies:
 - the recipients of the transferred personal data to which the BCRs apply;
 - the countries and territories to which the personal data may be transferred under the BCRs; and
 - the rights and obligations provided by the BCRs; or
- any other legally binding instrument.

The PDPR also recognizes the certification systems under the [Asia-Pacific Economic Cooperation \(APEC\) Cross-Border Privacy Rules \(CBPR\) System](#) and Privacy Recognition for Processors (PRP) System (see also the IMDA's [CBPR and Self-Assessment Form](#) and [PRP Requirements and Self-Assessment Form for Singapore](#)) as one of the modes for transfers of personal data overseas. A recipient is taken to have satisfied the requirements under the transfer limitation obligation if it is (Regulation 12 of the PDPR):

- receiving the personal data as an organization, and it holds a valid APEC CBPR certification; or
- receiving the personal data as a data intermediary, and it holds either a valid APEC PRP or CBPR certification, or both.

When are onward transfers from the initial recipient permitted?

The PDPA does not distinguish between cross-border data transfers carried out by data intermediaries and by organizations themselves. Hence, the same requirements under the Transfer Limitation Obligation would apply, and cross-border data transfers are permissible only when the overseas recipient is bound by legally enforceable obligations to provide the personal data transferred with a standard of protection comparable to that provided for by the PDPA. Please refer to the section on onward data transfers to third countries or international organizations above.

1.5. Accountability

Does the law ensure a high degree of accountability and awareness among controllers, processors, and data subjects?

Under the PDPA, organizations are required to undertake measures in order to ensure that they meet their obligations under the PDPA and demonstrate that they do so (Sections 11 and 12 of the PDPA) (the accountability obligation).

As part of the accountability obligation, organizations are required to appoint a data protection officer (DPO) and make available the business contact information of the DPO to the public. The DPO should have sufficient expertise and knowledge to be able to ensure that the organization complies with the PDPA.

Organizations are also required to develop and implement policies and practices that are necessary to meet the obligations under the PDPA and communicate to their staff information about these policies and practices.

Organizations must also develop processes to receive and respond to complaints that may arise with respect to the application of the PDPA and make information available to the data subjects regarding their data protection policies and practices and complaint process.

Controllers are also strongly advised to enter into a binding contract with their processor and clearly set out the scope of outsourcing and the attendant data protection obligations of the processor.

Additionally, the PDPC has issued a number of advisory guidelines and other publications to aid organizations in carrying out their obligations and to raise awareness among data subjects in relation to their rights under the PDPA. These advisory guidelines and other publications can be located on the PDPC's [website](#).

Does the law require data controllers and processors to demonstrate compliance to the competent supervisory authority?

A controller is responsible under the PDPA for the processing of personal data by their processor as if the personal data were processed by the controller themselves. In addition, the PDPA imposes the protection obligation and the retention limitation obligation directly on the processor. If the data processor has a reason to believe that a data breach has occurred in relation to the personal data it is processing on the controller's behalf, it should notify the data controller without undue delay.

In the event of a data breach, both the controller and the processor may be investigated by the PDPC, and either or both of them could be found in contravention of the PDPA.

Please also refer to the section on accountability and awareness in data controllers, processors, and subjects above on the accountability obligation under the PDPA.

1.6. What are the laws that enable public authorities to access transferred personal data held by private organizations?

There is no general legislation in Singapore that specifically relates to the surveillance conducted by public authorities of personal data held by private organizations. However, please see the section on the legal bases for public authorities to access and use personal data held by private organizations below for a discussion on the general powers accorded to the Singapore public authorities to access and seize data.

For completeness of understanding, the Singapore public agencies are not subject to the data protection provisions under the PDPA as they have their own set of data protection rules which all public officers must comply with. Public agencies are defined in the PDPA to include the Government, any ministry, department, agency, or organ of State, any tribunal appointed under any written law, or any specified statutory body. That said, this exclusion does not extend to organizations working on behalf of the Government agencies.

What are the general rules on access to transferred personal data for national security or law enforcement purposes?

Please see the sections on legal bases for public authorities to access and use personal data held by private organizations and limitations/safeguards to this legal basis below.

1.7. What legal bases are there for public authorities to access and use personal data held by private organizations?

There is no overarching legislation that specifically relates to the surveillance conducted by public authorities. Notwithstanding, there are certain laws in Singapore that empower Singapore authorities to access and seize data (which may include personal data), whether for domestic purposes or at the request of a foreign country. Depending on the laws in question, there are certain requirements and safeguards put in place in relation to the exercise of such power, for example, the requirement to obtain a court order.

Some of these statutory provisions, which allow Singapore authorities to do so, are discussed below.

CPC

Part IV of the [Criminal Procedure Code 2010 \(2020 Revised Edition\)](#) (CPC) gives authorities broad powers to seize relevant property, inspect computers (defined broadly to include, e.g., any data processing device), and access and decrypt data. For instance, Section 35(1) of the CPC allows a police officer to 'seize or prohibit the disposal of or dealing in any property:

- in respect of which an offence is suspected to have been committed;
- which is suspected to have been used or intended to be used to commit an offense; or
- which is suspected to constitute evidence of an offense.'

We also highlight that under Section 40 of the CPC, the [Public Prosecutor](#) may authorize a police officer to, for the purposes of investigating an arrestable offence, inter alia, 'require any person whom he reasonably suspects to be in possession of any decryption information [in relation to encrypted data under investigation] to grant him access to such decryption information as may be necessary to decrypt any data required for the purposes of investigating the arrestable offence.'

TA

Under the TA and other regulatory instruments, the IMDA is empowered to, by order, require any person to produce to the IMDA any document or information that the IMDA considers to be related to any matter relevant to an investigation or for discharging its functions under this Act (Section 78 of the TA).

Furthermore, telecommunications licensees may also be required, pursuant to the conditions of their license, to provide documents and information when requested by the IMDA.

OSA

Section 9 of the [Official Secrets Act 1935 \(2020 Revised Edition\)](#) (OSA) states that where it appears to the Minister that such a course is expedient in the public interest, they may, by warrant, require the owner or controller of any telecommunication system used for the sending or receipt of messages to or from any place out of Singapore, to produce such messages.

Prevention of Corruption Act

Section 22 of the [Prevention of Corruption Act 1960 \(2020 Revised Edition\)](#) (the Prevention of Corruption Act) allows the Director of the [Corrupt Practices Investigation Bureau](#) or any Magistrate, by warrant directed to any special investigator or police officer, to enter that place by force if necessary and to seize and detain any document or property, where there is reasonable cause to believe that it relates to the commission of a relevant offense.

MACMA

Separately, under the [Mutual Assistance in Criminal Matters Act 2000 \(2020 Revised Edition\)](#) (MACMA), the Singapore authorities are also empowered to assist certain foreign countries to, among other things, obtain evidence (e.g., data that is stored in a data center in Singapore), provided that the request is in respect of criminal matters.

Where an appropriate authority of a prescribed foreign country makes a request for the production of a thing or description of a thing for the purposes of any criminal matter in that country, the [Attorney General](#) may apply to the court for an order to (Section 22 of the MACMA):

- compel the production of the thing to an authorized officer for him to take away; or
- give an authorized officer access to the thing.

FICA

The [Foreign Interference \(Countermeasures\) Act 2021 \(No. 28 of 2021\)](#) (FICA), which has been brought into force progressively, introduces countermeasures to prevent, detect, and disrupt foreign interference in Singapore's domestic politics conducted through information campaigns and 'politically significant persons' (which includes political parties, members of the Parliament, etc.).

The FICA contains provisions that empower the competent authority to obtain information from organizations (which may potentially include personal information) regarding online communications activities that have been undertaken, or suspected of being, or having been undertaken, by or on behalf of a foreign principal.

Section 36 of FICA (which came into effect on July 7, 2022) provides for the issuance of a technical assistance direction by a competent authority on the order of the [Minister for Home Affairs](#) in response to online communications activities that, among other things, have been undertaken, or suspected of being or having been undertaken, by or on behalf of a foreign principal.

A technical assistance direction may require that a person to whom the direction is given to (which includes a provider of a relevant electronic service, an internet service with a Singapore link, or a hosting service, etc.) do one or more of the following:

- to provide information about whether any account maintained by the person for a customer is that for a foreigner;
- to provide technical information or other information about the person's relevant activity as specified in the direction; and/or
- to take any other step directed towards ensuring that the person is capable of giving help to the competent authority, which the competent authority requires in the public interest.

Section 108 of FICA (the entirety of which came into effect by December 29, 2023) empowers a competent authority to require any person (whether inside or outside Singapore) to provide information, documents, or material of any of the following, for specified purposes under Section 108(2) of FICA:

- the membership of the person by individuals who are not citizens of Singapore;
- relations with foreign principals;
- the provision of voluntary labor, or voluntary professional services, to or for the benefit of the person by individuals who are not citizens of Singapore; or
- recurrent and capital expenditure for the administration and management of activities undertaken by the person, which are directed towards a political end in Singapore.

The specified purpose under Section 108(2) of FICA is any matter which the competent authority considers necessary for determining whether any information provided to it under the FICA is correct, to determine whether there are grounds for any directive to be given under the FICA, and to determine whether or not to exercise any power under Parts 4, 5 or 6 of FICA.

1.8. Are there limitations/safeguards to the legal basis for access or use of personal data by public authorities?

Administrative action by a public authority may be subject to judicial review by the courts, provided that the relevant criteria are met.

While the data protection provisions of the PDPA do not apply to public agencies, we note that there are in place strict laws against the disclosure of official documents and information, which may contain the personal data of individuals. For e.g., under the OSA, criminal penalties are imposed on any person who wrongfully communicates confidential information that has been entrusted in confidence to him or her by government officeholders, or who fails to take reasonable care of such information by endangering the safety or secrecy of such information or otherwise.

In another example, the [Public Sector \(Governance\) Act 2018 \(2020 Revised Edition\)](#) (PSA) sets out directions regarding data sharing in the public sector and imposes criminal penalties on public officers who recklessly or intentionally disclose data (which may include personal data) without authorization, misuse data for a gain, or re-identify anonymized data.

Furthermore, the public sector has to comply with the Government's data security policies, such as the [Government Instruction Manual on Infocomm Technology & Smart Systems Management](#), which prescribes specific measures to manage and protect Government data, which includes personal data.

2. Existence and Functioning of Supervisory Authorities

2.1. Has an independent supervisory authority been established?

The PDPC has been appointed to be the body that oversees the protection of personal data in Singapore. The PDPC administers and enforces the PDPA and is empowered to issue directions (including administrative financial penalties) to private sector organizations that are in breach of the data protection provisions (e.g., where the disclosure of personal data is in contravention of the PDPA).

With effect from October 1, 2016, the PDPC was subsumed into the IMDA, which is a statutory body under the [Ministry of Communication and Information](#) (MCI).

In some sectors, organizations are also subject to the regulatory oversight of the relevant sectoral regulator (e.g., the IMDA for telecommunications licensees, and the MAS for financial institutions), which may administer and enforce certain legal obligations or regulatory requirements relating to privacy and data protection.

There is no privacy supervisory authority over public agencies *per se*. Nonetheless, there usually exist avenues to appeal decisions or determinations to the relevant Minister or the courts. Furthermore, as stated above, Singapore's administrative law provides for a judicial review mechanism that allows for the review of executive actions by the independent judiciary.

Is the supervisory authority completely independent and impartial?

As noted, the PDPC is responsible for the administration and enforcement of the PDPA, which covers activities relating to the collection, use, and disclosure of personal data in Singapore by private sector organizations. When performing any duty or exercising any power, it does so independently and in its own name. As a public authority whose administrative actions may ultimately be subject to judicial review by the courts, the PDPC is required to exercise its own mind on the exercise of its powers and not act under another's instruction. The PDPC's enforcement decisions are also subject to appeal to an independent appeal committee and the Singapore courts. Please see the sections on oversight mechanisms for public authorities and remedies for data subjects below.

In its [Guide on Active Enforcement](#) (revised October 1, 2022), the PDPC has expressly noted that one of its objectives is to maintain the trust between consumers and organizations by ensuring that appropriate enforcement actions are taken against organizations that are found to be in breach of the PDPA. When considering the appropriate enforcement action, the PDPC has noted that it is guided by four key objectives:

- to respond effectively to breaches of the PDPA where the focus is on those that adversely affect large groups of individuals and where the data involved are likely to cause harm or loss to the affected individuals;
- to be proportionate and consistent in the application of enforcement action on organizations that are found in breach of the PDPA;
- where penalties imposed serve as an effective deterrent to those that risk non-compliance to the PDPA; and
- to ensure that organizations that are found in breach take proper steps to correct gaps in the protection of personal data.

Does the supervisory authority function effectively, having adequate enforcement powers?

The PDPC has the following enforcement powers under the PDPA.

Powers of investigation

The Ninth Schedule of the PDPA sets out extensive powers of investigation of the PDPC and its inspectors, which include the power to:

- require the production of documents or information;

- require the provision of information (including requiring individuals to attend before the PDPC or inspector and provide statements); and
- enter premises with or without a court-issued search warrant.

Section 51 of the PDPA sets out certain offenses relating to, among others, obstructing or hindering the PDPC in the performance of any function or duty, or the exercise of any power, under the PDPA. It is also an offense for an organization or a person to, without reasonable excuse, neglect, or refuse to either provide any information or produce any document which the organization or person is required to provide or produce to the PDPC or an inspector, or attend before the PDPC or inspector as required.

Power to review

Under Section 48H of the PDPA, the PDPC may, among other things, review applications made by a complainant in relation to:

- a refusal by an organization to provide access to personal data or to correct personal data upon request, or failures to provide such access or correction within a reasonable time; or
- a fee required from the complainant by an organization in relation to an access or correction request by the complainant under the PDPA.

Upon completion of the review, the PDPC may:

- confirm the organization's refusal to provide access to or correct the personal data (as the case may be), or direct the organization to provide access to or correct the personal data (as the case may be) within a specified timeframe; or
- confirm, reduce, or disallow a fee, or direct the organization to make a refund to the complainant, as the case may be.

Power to issue directions and financial penalties

Under Section 48I of the PDPA, the PDPC may issue such directions as it thinks fit in the circumstances to ensure compliance by an organization with the PDPA. These include directions to:

- stop collecting, using, or disclosing personal data in contravention of the PDPA;
- destroy personal data collected in contravention of the PDPA; or
- comply with any direction of the PDPC.

The PDPC may also, if it is satisfied that an organization has intentionally or negligently contravened the data protection provisions in the PDPA, impose a financial penalty of up to SGD 1 million (approx. \$772,480) or 10% of the organization's annual turnover in Singapore, whichever is higher.

Voluntary undertakings

Section 48L of the PDPA empowers the PDPC to accept statutory undertakings. Where the PDPC has reasonable grounds to believe that an organization has not complied, is not complying, or is likely not to comply with any of the data protection provisions, the organization

may give, and the PDPC may accept, a written voluntary undertaking by the organization to take or refrain from taking specified action, as well as to publicize the voluntary undertaking.

Alternative dispute resolution

Section 48G of the PDPA empowers the PDPC to establish or approve one or more dispute resolution schemes for the resolution of complaints by mediation, and to make regulations relating to the operation of such schemes. The PDPC may, with or without the consent of the complainant and the organization, refer the matter to mediation under a dispute resolution scheme, or to resolve the complaint in a way directed by the PDPC.

Are there clear, precise, and accessible rules for the processing of personal data for surveillance/law enforcement purposes?

As mentioned in the section on demonstrating compliance to the competent supervisory authority above, the data protection provisions of the PDPA do not apply to public agencies.

However, as noted in the section on limitations/safeguards to the legal basis for access and use of personal data by public authorities above, public officers are subject to penalties under the PSA for offenses related to data protection, for e.g., for recklessly disclosing data without authorization, misusing data for gain, or reidentifying anonymized data.

2.2. What are the oversight mechanisms for the approval and review of relevant actions by public authorities?

Generally, there are a number of oversight mechanisms in place. Depending on the specific laws in question, these oversight mechanisms may include:

- the requirement for authorized officers to obtain court orders prior to requesting the production of material related to an investigation;
- avenues of appeal to the relevant Minister or designated appeal panel; and
- judicial review by the courts of administrative action or determinations by public bodies.

2.3. Are there legal remedies for data subjects, including effective individual rights and judicial redress?

The PDPA gives individuals the right to make access and correction requests. In summary, an organization must, upon request, allow an individual to access and/or correct their personal data in its possession or under its control. In addition, the organization is also obliged to provide the individual with information about the ways in which the personal data may have been used or disclosed during the past year (Sections 21 and 22 of the PDPA).

Moreover, individuals also have the right to withdraw their consent with respect to the collection, use, or disclosure of their personal data (Section 16 of the PDPA).

Individuals may lodge a complaint to the PDPC in respect of a contravention of the data protection provisions by an organization. In this regard, the PDPC has a broad range of enforcement powers, which include powers to review the refusal to provide access to personal data requested by the complainant, and the powers to issue directions or require the payment of a financial penalty.

From October 1, 2022, the PDPC is empowered to impose a financial penalty on organizations in breach of the data protection provisions in the PDPA, of up to a maximum of 10% of the organization's annual turnover in Singapore (if its annual turnover in Singapore exceeds SGD 10 million (approx. \$7,724,800)) or up to SGD 1 million (approx. \$772,480) in any other case. An organization's annual turnover in Singapore will be ascertained from the most recent audited accounts of the organization that are available at the time the financial penalty is imposed.

With respect to avenues of appeal under the PDPA, organizations and individuals aggrieved by certain decisions or directions by the PDPC may, within a specified time period, either apply to the PDPC for reconsideration or appeal to the Chairman of the Data Protection Appeal Panel (DPAP) as per the [Personal Data Protection \(Appeal\) Regulations 2021](#).

Appeals against, or with respect to, a direction or decision of the DPAP Committee may be made to the General Division of the High Court of Singapore (the High Court) on a point of law or as to the amount of a financial penalty (Section 48R(1) of the PDPA). The High Court shall hear and determine the appeal, and may (Section 48R(3) of the PDPA):

- confirm, modify, or reverse the direction or decision of the DPAP Committee; and
- make such further or other order on such appeal, whether as to costs or otherwise, as the High Court may think fit.

A decision of the High Court under Section 48R(3) of the PDPA may be further appealed to the Singapore Court of Appeal in accordance with the [Rules of Court 2021](#).

Individuals who have suffered loss or damage directly as a result of a contravention under the relevant provisions as stated in Section 48O of the PDPA may commence civil proceedings in the courts against the organization. If the PDPC has made a decision in respect of that contravention, the right of private action arises only after that decision by the PDPC becomes final as a result of there being no further right of appeal. The court hearing the action may grant the complainant an injunction or declaration, damages, and/or any other relief as the court thinks fit.

2.4. Can an organization refuse to comply with an authority access request and what remedies are available to them?

Under the PDPA, any disclosure of personal data by an organization without the individual's consent must be required or authorized under the PDPA or other written law.

Please see the section on legal remedies for data subjects above regarding remedies relating to public authorities' actions.

3. Additional Information

3.1. Do the above provisions apply to both residents/citizens of the jurisdiction and to foreign data subjects?

The PDPA does not make a distinction as to the nationality of data subjects. Furthermore, the PDPA applies to all private sector organizations, whether or not formed or recognized under Singapore law, or resident or having an office or place of business in Singapore.

3.2. Has the jurisdiction entered into international commitments or multilateral or regional systems?

Singapore has not signed or ratified any of the major international human rights treaties that uphold the right to privacy or data protection as a human right, such as the [International Covenant on Civil and Political Rights](#).

Nonetheless, Singapore has entered into non-legally binding international commitments relating to privacy and data protection, for instance, the APEC [Privacy Framework](#), which was developed in light of the 1980 [Organisation for Economic Co-operation and Development \(OECD\) Guidelines on the Protection of Privacy and Transborder Flows of Personal Data](#), and applies to all APEC member economies, including Singapore. The APEC Privacy Framework sets out principles and implementation guidance for public and private sectors that control the collection, holding, processing, use, transfer, or disclosure of personal information.

Singapore is also a participant in the APEC CBPR and the APEC PRP System. In June 2020, the [Personal Data Protection Regulations 2014](#) was amended to recognize the APEC CBPR and PRP system certifications for overseas transfers of personal data under the PDPA.

3.3. Is there any further information regarding public authorities' access to personal data held by private organizations?

No further information.