PANORAMIC

DATA PROTECTION & PRIVACY

Singapore

LEXOLOGY

Data Protection & Privacy

Contributing Editors

Aaron P Simpson and Lisa J Sotto

Hunton Andrews Kurth LLP

Generated on: July 19, 2024

Contents

Data Protection & Privacy

SHARING AND CROSS-BORDER TRANSFERS OF PI

RIGHTS OF INDIVIDUALS

EXEMPTIONS, DEROGATIONS AND RESTRICTIONS

SPECIFIC DATA PROCESSING

UPDATE AND TRENDS

Contributors

Singapore

Drew & Napier LLC

DREW & NAPIER

Lim Chong Kin chongkin.lim@drewnapier.com
Anastasia Su-Anne Chen anastasia.chen@drewnapier.com

LAW AND THE REGULATORY AUTHORITY

Legislative framework

Summarise the legislative framework for the protection of personal information (PI). Does your jurisdiction have a dedicated data protection law? Is the data protection law in your jurisdiction based on any international instruments or laws of other jurisdictions on privacy or data protection?

The main data protection legislation in Singapore is the Personal Data Protection Act 2012 (2020 Rev Ed) (PDPA).

The PDPA applies to all organisations that collect, use or disclose personal data in Singapore unless one of the exclusions under section 4 of the PDPA applies.

The PDPA recently underwent its first comprehensive review since its enactment in 2012. The Personal Data Protection (Amendment) Act 2020 (the Amendment Act), which was passed in Parliament on 2 November 2020, sets out extensive changes, the majority of which came into effect on 1 February 2021.

There are various regulations and advisory guidelines under the PDPA that deal with specific issues in greater detail. For example, the Personal Data Protection Regulations 2021 (the PDP Regulations) supplement the PDPA in four key areas:

- the requirements for transfers of personal data out of Singapore;
- the assessment relating to the processing of personal data in reliance on the grounds of deemed consent by notification and legitimate interests;
- the form, manner and procedures for making and responding to requests for access to or correction of personal data; and
- persons who may exercise rights concerning the disclosure of personal data of deceased individuals.

The other regulations issued under the PDPA include:

- the Personal Data Protection (Composition of Offences) Regulations 2021;
- the Personal Data Protection (Do Not Call Registry) Regulations 2013;
- the Personal Data Protection (Enforcement) Regulations 2021;
- the Personal Data Protection (Appeal) Regulations 2021; and
- the Personal Data Protection (Notification of Data Breaches) Regulations 2021.

The PDPC has issued several advisory guidelines and guides to provide greater clarity on the interpretation of the PDPA. The PDPC has also developed sector-specific advisory guidelines for:

- the telecommunications sector;
- the real estate agency sector;
- the education sector;

- the healthcare sector;
- the social services sector;
- transport services for hire (specifically concerning in-vehicle recordings); and
- for management corporations.

On 20 February 2018, Singapore became the sixth Asia-Pacific Economic Cooperation (APEC) economy to participate in the APEC Cross-Border Privacy Rules (CBPR) system. Singapore also became the second APEC economy to participate in the APEC Privacy Recognition for Processors (PRP) system. Collectively, the CBPR and PRP systems allow a smoother exchange of personal data among certified organisations in participating economies and ensure that data protection standards are maintained for consumers in the Asia-Pacific region.

The formulation of the PDPA framework has taken into account international best practices on data protection. As indicated during the second reading of the PDPA in Parliament in 2012, the then Minister of Information, Communications and the Arts had referred to the data protection frameworks in key jurisdictions such as Canada, New Zealand, Hong Kong and the European Union, as well as the Organisation for Economic Cooperation and Development Guidelines on the Protection of Privacy and Transborder Flows of Personal Data and the APEC Privacy Framework, in developing the PDPA framework.

Law stated - 16 May 2024

Data protection authority

Which authority is responsible for overseeing the data protection law? What is the extent of its investigative powers?

The PDPA is administered and enforced by the PDPC. With effect from 1 October 2016, the PDPC has been subsumed as a department under the Info-communications Media Development Authority (IMDA).

The PDPC may initiate an investigation to determine whether an organisation complies with the PDPA upon receipt of a complaint or on its own motion.

According to the Advisory Guidelines on Enforcement of Data Protection Provisions, the factors that the PDPC may consider in deciding whether to commence an investigation include:

- whether the organisation may have failed to comply with all or a significant part of its obligations under the PDPA;
- whether the organisation's conduct indicates a systemic failure by the organisation to comply with the PDPA or to establish and maintain the necessary policies and procedures to ensure its compliance;
- the number of individuals who are, or may be, affected by the organisation's conduct;
- the impact of the organisation's conduct on the complainant or any individual who may be affected;
-

whether the organisation had previously contravened the PDPA or may have failed to implement the necessary corrective measures to prevent the recurrence of a previous contravention;

- where the complainant had previously approached the organisation to seek a resolution of the issues but failed to reach a resolution;
- where the PDPC has sought to facilitate dispute resolution between the complainant and the organisation, whether the complainant and the organisation agreed to participate in the dispute resolution process, their conduct during the dispute resolution process and the outcome of the dispute resolution process;
- where a review has been commenced by the PDPC, whether the organisation has complied with its obligations under the Enforcement Regulations in relation to a review, the organisation's conduct during the review and the outcome of the review; and
- public interest considerations.

In the course of its investigation, the PDPC's powers include:

- requiring any organisation to produce any specified document or to provide any specified information;
- compelling the attendance of witnesses, the provision of information and the production of documents;
- entering an organisation's premises without a warrant (by giving at least two working days' advance notice of intended entry); and
- obtaining a search warrant to enter an organisation's premises and search the premises or any person on the premises (if there are reasonable grounds for believing that he or she has in his or her possession any document, equipment or article relevant to the investigation), and take possession of, or remove, any document, equipment or article relevant to an investigation.

The PDPC is also empowered to review complaints concerning access and correction requests.

Law stated - 16 May 2024

Cooperation with other data protection authorities

Are there legal obligations on the data protection authority to cooperate with other data protection authorities, or is there a mechanism to resolve different approaches?

The PDPC may enter into a cooperation agreement with a foreign data protection authority for data protection matters such as cross-border cooperation. Cooperation may take the form of information exchange or any other assistance as necessary to assist in the enforcement or administration of data protection laws.

Specifically, section 10 of the PDPA provides that the cooperation agreement has to be entered into for the purposes of:

- facilitating cooperation between the PDPC and another foreign data protection authority in the performance of their respective functions insofar as those functions relate to data protection; and
- avoiding duplication of activities by the PDPC and another foreign data protection authority, being activities involving the enforcement of data protection laws.

In this regard, the cooperation agreement may include provisions to:

- enable the PDPC and the other foreign data protection authority to furnish to each other information in their respective possession if the information is required by the other for the purpose of performance by it of any of its functions;
- provide such other assistance to each other as will facilitate the performance by the other of any of its functions; and
- enable the PDPC and the other foreign data protection authority to forbear to perform any of their respective functions concerning a matter in circumstances where it is satisfied that the other is performing functions concerning that matter.

Under the PDPA, the PDPC may only furnish information to a foreign data protection authority pursuant to a cooperation agreement if it obtains from that authority an undertaking in writing that it will comply with terms specified in that agreement, including terms that correspond to the provisions of any written law concerning the disclosure of that information by the PDPC.

In particular, where the information requested contains personal data that is treated as confidential under the PDPA, the PDPA specifies that the PDPC may only disclose the information to the foreign data protection authority if the following conditions are met:

- the information or documents requested by the foreign data protection authority are in the possession of the PDPC;
- unless the government otherwise allows, the foreign data protection authority undertakes to keep the information confidential at all times; and
- the disclosure of the information is not likely to be contrary to the public interest.

The PDPC is also a participant in the Asia Pacific Economic Corporation Cross-border Privacy Enforcement Arrangement (APEC CPEA), which creates a framework for the voluntary sharing of information and provision of assistance for privacy enforcement-related activities.

Law stated - 16 May 2024

Breaches of data protection law

Can breaches of data protection law lead to administrative sanctions or orders, or criminal penalties? How would such breaches be handled?

Generally, the enforcement powers of the PDPC include:

- powers to direct alternative dispute resolution (ADR);
- powers to review (in respect of access or correction requests); and
- powers of investigation.

Any individual affected by an organisation's non-compliance with the PDPA may lodge a complaint with the PDPC. Upon receipt of a complaint, the PDPC may investigate or review the matter, or direct the parties as to the appropriate mode of dispute resolution.

Concerning ADR, under section 48G(1) of the PDPA, the PDPC is provided with the power to establish or approve one or more dispute resolution schemes, and direct complainants to resolve disputes via mediation, without the need to secure the consent of both parties.

As to the type of enforcement action it may take, the PDPC may choose to do any one of the following:

- suspend or discontinue an investigation;
- accept a voluntary undertaking;
- initiate a full investigation; or
- issue an expedited decision.

The PDPA also provides that a person may be guilty of a criminal offence in certain circumstances.

Suspend or discontinue an investigation

The PDPC may discontinue investigations and simply issue an advisory notice where the impact is assessed to be low. Section 50(3) of the PDPA sets out circumstances in which the PDPC may do so, including where a complainant has not complied with a direction, the parties involved have mutually agreed to settle, or any party has commenced legal proceedings in respect of any contravention of the PDPA.

Voluntary undertaking

A voluntary undertaking is a written agreement between the organisation and the PDPC, in which the organisation voluntarily commits to remedy the breaches and take steps to prevent a recurrence. The organisation's request to invoke the undertaking process must be made very soon after the incident is known. The PDPC has sole discretion to accept or reject a voluntary undertaking. The PDPC is unlikely to accept an undertaking request in certain cases (eg, where the organisation refutes responsibility for the data breach incident, or where it is a repeat incident entailing a similar cause of the breach).

Section 48L of the PDPA empowers the PDPC to accept statutory undertakings from an organisation when the PDPC has reasonable grounds to believe that an organisation has not complied, is not complying or is likely not to comply with the PDPA.

Where an organisation is found not to have complied with any term of the voluntary undertaking, the PDPC may take action that it thinks fit in the circumstances, which may include issuing directions and imposing available enforcement remedies.

Full investigation process

For incidents with high impact, and where facilitation or mediation is inappropriate in the circumstances (eg, where there is a disclosure of personal data on a large scale or where the personal data disclosed could cause significant harm), the PDPC may initiate a full investigation.

Where the PDPC is satisfied that an organisation has intentionally or negligently contravened the PDPA, it is empowered with wide discretion to issue such remedial directions as it thinks fit. These include directions requiring the organisation to:

- stop collecting, using or disclosing personal data in contravention of the PDPA;
- destroy personal data collected in contravention of the PDPA;
- provide access to, correct or port personal data, or reduce or make a refund of any fee charged for any access, porting or correction request; or
- pay a financial penalty of up to a maximum of 10 per cent of the organisation's annual turnover in Singapore, or S$1 million, whichever is higher.

Expedited decision procedure

The PDPC may issue an expedited breach decision at its discretion where the organisation makes an upfront, voluntary admission of liability for breaching the PDPA. The expedited decision procedure allows investigations to be completed in a significantly shorter time, compared to a full investigation. The organisation's admission of its role in the incident would also be considered favourably by the PDPC, in determining the financial penalty to be imposed. However, admissions are unlikely to be considered as a strong mitigating factor for repeated data breaches. The organisation must make a written request to the PDPC for an expedited decision very soon after the incident is known to the organisation.

Criminal offences

Part 9B of the PDPA sets out offences relating to the egregious mishandling, by individuals, of personal data in the possession of or under the control of an organisation or a public agency. In particular, it is an offence:

- under section 48D, if an individual discloses, or causes the disclosure of, personal data in the possession or control of an organisation or a public agency to another person, which is not authorised, and the individual does so knowingly or is reckless to the disclosure not being authorised;
- under section 48E, if an individual makes use of personal data in the possession or control of an organisation or a public agency which is not authorised, the individual does so knowingly or is reckless to the use not being authorised, and as a result of the use of the personal data, the individual:

- obtains a gain;
- causes harm to another individual; or
- causes loss to another person, that individual shall be guilty of an offence;

- under section 48F, if an individual takes any action to reidentify or cause the reidentification of anonymised information in possession or control of an organisation or a public agency, which is not authorised, and the individual does so knowingly or is reckless to the re-identification not being authorised.

The penalty for these offences is a fine not exceeding S$5,000 or imprisonment for a term not exceeding two years, or both. However, certain defences are provided for in respect of these offences, for example, where the accused used, disclosed or reidentified the data in the reasonable belief that the accused had the legal right to do so, and was not reckless as to whether this was so.

Section 51 of the PDPA also sets out certain offences 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 offence for an organisation or a person, without reasonable excuse, to neglect or refuse to either provide any information or produce any document that the organisation or person is required to provide or produce to the PDPC or an inspector or attend before the PDPC or inspector as required.

Law stated - 16 May 2024

Judicial review of data protection authority orders

Can PI owners appeal to the courts against orders of the data protection authority?

With respect to avenues of appeal under the PDPA, organisations and individuals aggrieved by enforcement decisions or directions of the PDPC may, within a specified time period, either apply to the PDPC for reconsideration or appeal to the chair of the Data Protection Appeal Panel (per the Personal Data Protection (Appeal) Regulations 2021).

Appeals against a direction or decision of a Data Protection Appeal Committee may be made to the General Division of the High Court, in respect of a point of law or as to the amount of a financial penalty (section 48R(1) of the PDPA). The High Court may then confirm, modify or reverse the direction or decision of the Appeal Committee, and make a further or other order on such appeal, whether as to costs or otherwise (section 48R(3) of the PDPA). A decision of the High Court under section 48R(3) of the PDPA may be further appealed to the Court of Appeal in accordance with the Rules of Court.

As a public authority, any administrative action by the PDPC may also be subject to judicial review by the courts, provided that the relevant thresholds and conditions are met (eg, exhaustion of other possible alternative remedies).

Law stated - 16 May 2024

SCOPE

Exempt sectors and institutions

Does the data protection law cover all sectors and types of organisation or are some areas of activity outside its scope?

The Personal Data Protection Act 2012 (PDPA) applies to all private sector organisations in Singapore, regardless of their scale or size.

An 'organisation' is defined broadly under the PDPA as including any individual, company, association or body of persons, corporate or unincorporated, and whether or not formed or recognised under the law of Singapore, or resident or having an office or place of business in Singapore.

Section 4 of the PDPA provides that the data protection provisions of the PDPA (ie, Parts 3 to 6B of the PDPA) do not impose any obligation on:

- individuals acting in a personal or domestic capacity;
- employees acting in the course of their employment with an organisation (although employees may be liable for the egregious mishandling of personal data in the possession of or under the control of an organisation or a public agency); and
- public agencies.

The PDPA is intended to set a baseline standard for personal data protection across the private sector, and will operate alongside (and not override) existing laws and regulations. Section 4(6) of the PDPA provides that the PDPA does not affect any right or obligation under the law and that in the event of any inconsistency, the provisions of other written laws will prevail.

Law stated - 16 May 2024

Interception of communications and surveillance laws

Does the data protection law cover interception of communications, electronic marketing or monitoring and surveillance of individuals?

To the extent that personal data is collected, used or disclosed in the interception of communications and in the monitoring and surveillance of individuals, the PDPA applies to any private sector organisation collecting, using or disclosing such data. As such, the individual's prior consent is required before any collection takes place unless an exception to consent applies or the collection is otherwise authorised under law.

As such, where the provisions under other legislation require or authorise the interception of communications and the monitoring and surveillance of individuals, this would prevail to the extent of inconsistency with the consent obligation under the PDPA. Below is a non-exhaustive list of such provisions:

- Organisations providing telecommunications services and holding services-based operations licences may have to comply with interception requests by the IMDA and other authorities. Specifically, condition 16.2 of the IMDA's standard Services-Based Operator (Individual) (SBO (I)) licence conditions expressly permits disclosure of

subscriber information where the disclosure of subscriber information is deemed necessary to the IMDA or such other relevant law enforcement or security agencies in the exercise of their functions or duties. Condition 26.1 of the IMDA's standard SBO (I) licence conditions also requires licensees to 'provide the [IMDA] with any document and information within its knowledge, custody or control, which the [IMDA] may, by notice or direction require'.

- Section 20 of the Criminal Procedure Code 2010 (2020 Rev Ed) empowers the police to require the production of a 'document or other thing' (which is necessary or desirable for any investigation, inquiry, trial or another proceeding under the Code) by issuing a written order to the 'person in whose possession or power the document or thing is believed to be'.
- Section 10 of the Kidnapping Act 1961 (2020 Rev Ed) states that the Public Prosecutor may authorise any police officer to, among others, 'intercept any message transmitted or received by telecommunication' or 'intercept or listen to any conversation by telephone', if it is likely to contain information relating to payment of ransom for release of someone who had been kidnapped.
- Section 19 of the Cybersecurity Act 2018 (2020 Rev Ed) (the Cybersecurity Act) states that where information regarding a cybersecurity threat or incident has been received by the Commissioner, he or she may exercise certain powers as are necessary to investigate the cybersecurity threat or incident, including the power to require the provision of any document in a person's possession or information considered to be related to the matter.

Electronic marketing

Generally, where the personal data of an individual is collected, used and disclosed for marketing purposes, the consent of the individual concerned must be obtained. Further, such consent must not have been obtained as a condition for the provision of a product or service where it would not be reasonably required to provide that product or service. Deemed consent by notification also does not apply to personal data used for marketing purposes. More generally, the Personal Data Protection Commission (PDPC) has noted in its Advisory Guidelines on Key Concepts in the Personal Data Protection Act (revised 16 May 2022) (Key Concepts Guidelines) that a failure to opt out will not be regarded as appropriate for obtaining consent for marketing purposes, and recommended that organisations obtain consent from an individual through a positive action of the individual (eg, opt-in consent).

Concerning the sending of marketing communications by telephone call or text messaging (or fax) to a Singapore telephone number, Part 9 of the PDPA (ie, the Do Not Call (DNC) provisions) requires an organisation to:

- obtain valid confirmation that the telephone number is not listed on the relevant DNC Register before sending the message or call, unless clear and unambiguous consent to the sending of the specified message to that number is obtained in evidential form;
- include in the specified message information identifying the sender of the messages and details on how the sender can be readily contacted, and such details and contact information should be reasonably likely to be valid for at least 30 days after the sending of the message; and

- for voice calls, not conceal or withhold the calling line identity from the recipient.

A limited exception exists concerning sending messages to individuals with whom the organisation has an ongoing relationship.

Concerning the duty to check the DNC Registry, section 43A of the PDPA imposes obligations on third-party checkers to communicate accurate DNC Register query results to the organisations that they are checking the DNC Register on behalf of.

Further, Part 9A of the PDPA contains a prohibition concerning the sending of applicable messages to telephone numbers generated or obtained through the use of dictionary attacks and address-harvesting software.

The DNC provisions (which used to be enforced as criminal offences) are now enforced under the same administrative regime as the data protection provisions. If the organisation is found to have intentionally or negligently contravened any provision of Part 9, the PDPC may impose a financial penalty not exceeding:

- S$200,000, in the case of an individual; or
- S$1 million, in any other case.

If the organisation is found to have intentionally or negligently contravened any provision of Part 9A, the PDPC may impose a financial penalty not exceeding:

- S$200,000, in the case of an individual;
- 5 per cent of the person's annual turnover in Singapore, where the person's annual turnover in Singapore exceeds S$20 million; or
- S$1 million, in any other case.

Complementing the DNC provisions of the PDPA, the Spam Control Act 2007 (2020 Rev Ed) (the Spam Control Act) regulates the bulk sending of unsolicited commercial electronic messages to email addresses or mobile telephone numbers.

Section 11, read with the Second Schedule of the Spam Control Act, requires any person who 'sends, causes to be sent or authorises the sending of unsolicited commercial electronic messages (which includes emails, instant messages (on platforms such as Telegram and WeChat) and short message service or multimedia message service) in bulk' to comply with certain obligations. These include, among others, requirements that unsolicited commercial electronic messages must contain:

- an unsubscribe facility;

the label '' to indicate that the message is an advertisement; and

- the message must not contain header information that is false or misleading.

Section 9 of the Spam Control Act also prohibits electronic messages from being sent to electronic addresses generated or obtained through the use of a dictionary attack or address-harvesting software.

The Spam Control Act provides for civil liability (including the grant of an injunction or the award of damages) against parties in breach of these requirements. Statutory damages of

up to S$25 per message may be awarded, up to an aggregate of S$1 million (unless the plaintiff proves that his or her actual loss is higher).

Law stated - 16 May 2024

Other laws

Are there any further laws or regulations that provide specific data protection rules for related areas?

Various other laws and regulations in Singapore set out data protection-related rules, some of which are sector-specific. For instance:

- the Banking Act 1970 (2020 Rev Ed) prescribes the disclosure of customer information by a bank or its officers;
- the Computer Misuse Act 1993 (Rev Ed) deals with computer system hackers and other similar forms of unauthorised access or modification to computer systems;
- the Cybersecurity Act 2018 (2020 Rev Ed) establishes a legal framework for the oversight and maintenance of national cybersecurity in Singapore to ensure that computers, systems and data are better protected;
- the Healthcare Services Act 2020 (No. 3 of 2020), which replaces the Private Hospitals and Medical Clinics Act (Cap 248), contains provisions relating to the confidentiality of information held by healthcare service providers licensed under the Act;
- the Official Secrets Act 1935 (2020 Rev Ed) contains provisions relating to the prevention of disclosure of official documents and information;
- the Public Sector (Governance) Act 2018 (2020 Rev Ed) sets out directions for data sharing among government agencies and imposes criminal penalties on public officers who recklessly or intentionally disclose data without authorisation, misuse data for a gain or reidentify anonymised data; and
- the Telecom and Media Competition Code issued under the Telecommunications Act 1999 (2020 Rev Ed) contains certain provisions pertaining to the safeguarding of end-user service information.

Concerning the financial sector, the Monetary Authority of Singapore (MAS) is empowered under the Monetary Authority of Singapore Act 1970 (2020 Rev Ed) and other sectoral legislation to issue directives and notices. Examples of MAS-issued regulatory instruments that are relevant to data protection include the Notices on Cyber Hygiene, Notices and Guidelines on Technology Risk Management, Notices and Guidelines on Prevention of Money Laundering and Countering the Financing of Terrorism, and the Guidelines on Outsourcing. These regulations operate alongside the PDPA and prevail to the extent of any inconsistency.

Law stated - 16 May 2024

PI formats

What categories and types of PI are covered by the law?

All formats of personal information are covered under the PDPA, whether electronic or non-electronic and regardless of the degree of sensitivity. 'Personal data' is broadly defined under the PDPA as data, whether true or not, about an individual who can be identified from that data, or from that data and other information to which the organisation has or is likely to have access.

Nonetheless, the PDPA provides for certain exceptions and limitations as to its applicability. For example, the PDPA does not apply to personal data that is contained in a record that has been in existence for at least 100 years. The data protection provisions of the PDPA also do not apply to 'business contact information' as defined under the PDPA.

Law stated - 16 May 2024

Extraterritoriality

Is the reach of the law limited to PI owners and processors physically established or operating in your jurisdiction, or does the law have extraterritorial effect?

The data protection provisions apply to all organisations that collect, use or disclose personal data in Singapore, regardless of whether they are formed or recognised under Singapore law or whether they are resident or have an office or place of business in Singapore. As such, organisations that are located overseas are still subject to the data protection provisions as long as they collect, use or disclose personal data in Singapore. Also, organisations that collect personal data overseas and host or process it in Singapore will be subject to the relevant obligations under the PDPA from the point that such data is brought into Singapore.

Law stated - 16 May 2024

Covered uses of PI

Is all processing or use of PI covered? Is a distinction made between those who control or own PI and those who provide PI processing services to owners? Do owners', controllers' and processors' duties differ?

Yes, the PDPA regulates all collection, use, disclosure and processing of personal data by an organisation.

However, the PDPA imposes fewer obligations directly on a 'data intermediary'. A data intermediary refers to an organisation that processes personal data on behalf of and for the purposes of another organisation (the primary organisation) pursuant to a written contract.

A data intermediary is only required to comply with the obligations relating to:

- the protection of personal data (section 24);
- the retention of personal data (section 25); and
- the duty to notify the primary organisation without undue delay where it has reason to believe that a data breach has occurred concerning personal data that it is processing on the primary organisation's behalf (sections 26C(3)(a) and 26E).

A data intermediary that processes personal data in a manner that goes beyond the processing required under the written contract would not be considered a data intermediary and is subject to the full suite of data protection provisions under the PDPA in respect of that processing.

Law stated - 16 May 2024

LEGITIMATE PROCESSING OF PI

Legitimate processing – grounds

Does the law require that the processing of PI be legitimised on specific grounds, for example to meet the owner's legal obligations or if the individual has provided consent?

Yes, an individual's consent is required before an organisation can collect, use or disclose such individual's personal data, unless otherwise required or authorised by law. Such consent must be validly obtained and may be either expressly given or deemed to have been given.

For consent to be considered validly obtained the organisation must first inform the individual of the purposes for which his or her personal data will be collected, used or disclosed. These purposes have to be what a reasonable person would consider appropriate in the circumstances.

Consent obtained via the following ways does not constitute valid consent for the purpose of the PDPA:

- 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, to obtain or attempt to obtain the individual's consent.

The PDPA stipulates that consent is deemed to have been given in certain circumstances, specifically:

- Deemed consent by conduct: where an individual voluntarily provides his or her personal data to the organisation for a particular purpose, and it is reasonable that the individual would voluntarily provide his or her personal data.
- Deemed consent by contractual necessity:
    - in a situation where an individual who provides personal data to organisation A with a view to enter into a contract with organisation A – where the disclosure of personal data from organisation A to organisation B is reasonably necessary for the conclusion or performance of a contract or transaction between the individual and organisation A. This deemed consent by contractual necessity also extends to disclosure by organisation B to another downstream organisation C where the disclosure by organisation B (and collection by organisation C) is reasonably necessary to fulfil the contract between the individual and organisation A; or

- in a situation where an individual enters into a contract with organisation A and provides personal data to organisation A pursuant or in relation to that contract – where the disclosure of personal data from organisation A to organisation B is reasonably necessary for the performance of the contract between the individual and organisation A; or for the conclusion or performance of a contract between organisation A and organisation B which is entered into at the individual's request, or which a reasonable person would consider to be in the individual's interest. This deemed consent by contractual necessity also extends to disclosure by organisation B to another downstream organisation C where the disclosure by organisation B is reasonably necessary for the performance of the contract between the individual and organisation A; or for the conclusion or performance of a contract between organisation A and organisation B entered into at the individual's request, or which a reasonable person would consider to be in the individual's interest.

- Deemed consent by notification: subject to the organisation's fulfilment of preconditions such as the conduct of an assessment to determine that the proposed processing of personal data is not likely to have an adverse effect, an individual may be deemed to have consented to the organisation's collection, use or disclosure of his or her personal data for a purpose that he or she has been notified of. The organisation must provide a reasonable period for the individual to opt out before it 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 and the individual did not notify the organisation to opt out.

While consent is generally required, the First and Second Schedules to the PDPA provide for specific situations where personal data can be collected, used or disclosed without the individual's consent. Such exceptions to consent include those relating to:

- vital interests of individuals;
- public interests;
- legitimate interests;
- business asset transactions;
- business improvement purposes; and
- research.

Law stated - 16 May 2024

Legitimate processing – types of PI

Does the law impose more stringent rules for processing specific categories and types of PI?

The PDPA does not expressly prescribe a different set of rules for specific categories of personal data. However, as a number of the data protection provisions adopt a standard of reasonableness, the sensitivity of the personal data in question could, in practice, affect the measures that an organisation must put in place to ensure compliance.

For instance, section 24 of the PDPA requires that an organisation would need to make 'reasonable security arrangements' to protect personal data in its possession or under its control, to prevent:

- unauthorised 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.

The Personal Data Protection Commission (PDPC) has emphasised that organisations should take into account the sensitivity and volume of personal data when deciding on the appropriate level of security arrangements needed to protect it.

Notably, the PDPC also imposes more stringent guidelines concerning National Registration Identity Card (NRIC) numbers and other national identification numbers. According to the Advisory Guidelines on the PDPA for NRIC and other National Identification Numbers (issued on 31 August 2018), organisations are generally not allowed to collect, use or disclose NRIC numbers and other national identification numbers unless such collection, use or disclosure is required under the law (or an exception under the PDPA applies), or is necessary to accurately establish or verify the identity of the individual to a high degree of fidelity.

Law stated - 16 May 2024

DATA HANDLING RESPONSIBILITIES OF OWNERS OF PI

Transparency

Does the law require owners of PI to provide information to individuals about how they process PI? What must the notice contain and when must it be provided?

The obligation to notify individuals stems primarily from the process of seeking valid consent for the processing of personal data. In particular, organisations are obliged to inform individuals of:

- the purposes for the collection, use or disclosure of his or her personal data, on or before collecting the personal data;
- any other purpose for the use or disclosure of personal data that has not been notified to the individual (under the previous bullet point), before such use or disclosure of personal data; and
- on request by the individual, the business contact information of a person who can answer the individual's questions about the collection, use or disclosure of the personal data on behalf of the organisation.

Only after the above information has been notified to the individual can he or she be considered to have validly given his or her consent to the collection, use or disclosure of his or her personal data for such purposes.

While the Personal Data Protection Act 2012 (PDPA) requires that such notice be provided to the individual on or before the collection, use and disclosure of his or her personal data,

there is no prescribed manner or form in which such a notice must be given. Per the Advisory Guidelines on Key Concepts in the PDPA, it is good practice for the organisation to 'state its purposes in a written form'.

More generally, the PDPA requires that an organisation makes information available on request about its data protection policies and practices. This would typically be satisfied through an external data protection notice.

Law stated - 16 May 2024

Exemptions from transparency obligations

When is notice not required?

The First and Second Schedules to the PDPA set out respectively certain circumstances where an individual's consent need not be obtained for the collection, use and disclosure of his or her personal data. Accordingly, the requirement to notify the individual would generally not apply under such circumstances.

However, section 20(4) of the PDPA is an exception to the rule. Where an organisation intends to collect, use or disclose personal data for the purpose of, or in relation to, the organisation:

- entering into an employment relationship with the individual or appointing him or her to any office; or
- managing or terminating an employment relationship with, or appointment of, the individual,

the organisation must notify the individual of that purpose on or before such collection, use or disclosure (despite the fact that there is no requirement to seek consent).

Similarly, where an organisation intends to collect, use or disclose personal data by relying on the 'legitimate interests' exception, the PDPA requires the organisation to disclose its reliance.

Law stated - 16 May 2024

Data accuracy

Does the law impose standards in relation to the quality, currency and accuracy of PI?

Yes, section 23 of the PDPA generally requires that organisations make a reasonable effort to ensure that the personal data they collect is accurate and complete if the personal data is likely to be used by the organisation to make a decision that affects the individual or is likely to be disclosed by the organisation to another organisation. This is regardless of whether the personal data is collected directly by the organisation or on behalf of the organisation.

The Personal Data Protection Commission (PDPC), in its Key Concepts Guidelines, has stated that an organisation must make a reasonable effort to ensure that:

-

it accurately records the personal data it collects (whether directly from the individual concerned or through another organisation);

- the personal data it collects includes all relevant parts thereof (so that it is complete);
- it has taken the appropriate (reasonable) steps in the circumstances to ensure the accuracy and correctness of the personal data; and
- it has considered whether it is necessary to update the information.

Law stated - 16 May 2024

Data minimisation

Does the law restrict the types or volume of PI that may be collected?

The PDPA does not specifically restrict the types or volume of personal information (PI) that may be collected. However, section 18 of the PDPA provides that organisations may collect, use or disclose personal data only for purposes that a reasonable person would consider appropriate.

Further, the PDPC clarified in its Advisory Guidelines on the PDPA for the National Registration Identity Card (NRIC) and other National Identification Numbers (issued on 31 August 2018), that to comply with section 18 of the PDPA, organisations generally must not collect, use or disclose NRIC numbers and other national identification numbers unless such collection, use or disclosure is required under the law (or pursuant to an exception under the PDPA), or is necessary to accurately establish or verify the identity of the individual to a high degree of fidelity.

Law stated - 16 May 2024

Data retention

Does the law restrict the amount of PI that may be held or the length of time for which PI may be held?

Yes, section 25 of the PDPA provides that organisations (including data intermediaries) should cease to retain personal data, or remove how it can be associated with particular individuals, as soon as it is reasonable to assume that such retention no longer serves the purposes for which the data was collected, and retention is no longer necessary for legal or business purposes. Such legal or business purposes may, for example, include situations where the personal data is required for an ongoing legal action involving the organisation, where retention of the personal data is necessary to comply with the organisation's obligations under other applicable laws, or where the personal data is required for an organisation to carry out its business operations, such as to generate annual reports or performance forecasts.

Law stated - 16 May 2024

Purpose limitation

Are there any restrictions on the purposes for which PI can be used by owners? If there are purpose limitations built into the law, how do they apply?

Yes, the purposes for which personal data can be used or disclosed by organisations are restricted to the purposes for which the individual concerned has been informed of and given his or her consent (if applicable). Further, an organisation may collect, use or disclose personal data about an individual only for purposes that a reasonable person would consider appropriate in the circumstances.

Generally, fresh consent would need to be obtained where organisations are seeking to collect, use or disclose personal data for different purposes from those to which the individual concerned had given his or her consent, unless there is an applicable exception.

Law stated - 16 May 2024

Automated decision-making

Does the law restrict the use of PI for making automated decisions without human intervention that affect individuals, including profiling?

The PDPA does not specifically restrict the use of PI for making automated decisions, including profiling. However, the PDPA's general data protection obligations would apply insofar as there is any collection, use or disclosure of personal data for such purpose (such as the obligation to obtain consent and to use personal data only for purposes that a reasonable person would consider appropriate).

In its Advisory Guidelines on the Use of Personal Data in AI Recommendation and Decision Systems (issued on 1 March 2024), the PDPC highlighted that when organisations deploy artificial intelligence (AI) systems in their services or products that collect or use personal data to provide new functionalities or enhance product features, they should be mindful of the consent (sections 13 to 17 of the PDPA), notification (section 20 of the PDPA) and accountability (sections 11 and 12 of the PDPA) obligations.

The consent and notification obligations are complementary to one another. Combined, they require that users be notified of the purpose of the collection and intended use of their personal data when seeking their consent. Consent obtained by organisations should be meaningful, and notification provided involves providing information about the types of personal data that will be collected and processed and the purpose of the processing. Organisations should place themselves in the shoes of consumers and craft notifications that will enable individuals to understand how their personal data will be processed to achieve the intended purpose.

In this regard, the PDPC encourages organisations to provide the following information in their notifications (to the extent practicable):

- the function of their product that requires the collection and processing of personal data;
- a general description of the types of personal data that will be collected and processed;

- an explanation of how the processing of collected personal data is relevant to the product feature; and
- the specific features of personal data that are more likely to influence the product feature.

If an organisation assesses that it is necessary to limit or omit details and provide a more general explanation due to commercial sensitivity or to protect the security of its AI systems, it should clearly document its justifications for such decision internally.

With regard to an organisation's accountability obligation, the PDPC states that organisations that make use of AI systems should be transparent and include in their written policies relevant practices and safeguards to achieve fairness and reasonableness. The level of detail provided should be proportionate to the risks in each use case (eg, taking into account the potential harm to the individual and the level of autonomy of the AI system).

Law stated - 16 May 2024

SECURITY

Security obligations

What security obligations are imposed on PI owners and service providers that process PI on their behalf?

Section 24 of the Personal Data Protection Act 2012 (PDPA) requires that organisations protect the personal data in their possession or control by making 'reasonable security arrangements' to prevent:

- unauthorised 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.

Organisations that process personal data on behalf of an organisation (ie, data intermediaries) are also subject to the same requirement.

While the Personal Data Protection Commission (PDPC) recognises that there is no one-size-fits-all solution in respect of the type of security arrangements, it has, in its Key Concepts Guidelines, advised organisations to:

- design and organise their security arrangements to fit the nature and form of the personal data held by the organisation and the possible harm that might result from a security breach;
- identify reliable and well-trained personnel responsible for ensuring information security;
- implement robust policies and procedures for ensuring appropriate levels of security for personal data of varying levels of sensitivity; and
- be prepared and able to respond to information security breaches promptly and effectively.

Further, the PDPC's Guide to Data Protection Practices for Information and Communications Technology (ICT) systems sets out good practices concerning ICT security measures that organisations should adopt to protect electronic personal data (eg, concerning ICT security audits and tests, authentication and authorisation, computer networks and email security).

Law stated - 16 May 2024

Notification of data breach

Does the law include (general or sector-specific) obligations to notify the supervisory authority or individuals of data breaches? If breach notification is not required by law, is it recommended by the supervisory authority?

Yes, the relevant provisions may be found in Part 6A of the PDPA. Under section 26A of the PDPA, a 'data breach', concerning personal data, is defined as:

- the unauthorised access, collection, use, disclosure, copying, modification or disposal of personal data; or
- the loss of any storage medium or device on which personal data is stored in circumstances where the unauthorised access, collection, use, disclosure, copying, modification or disposal of the personal data is likely to occur.

Under section 26B of the PDPA, a data breach is a 'notifiable data breach' if it:

- results in, or is likely to result in, significant harm to any individual to whom any personal data affected by a data breach relates; or
- is, or is likely to be, of a significant scale (ie, 500 or more individuals).

A data breach is deemed to result in significant harm to an individual if it affects any prescribed class of personal data under the Personal Data Protection (Notification of Data Breaches) Regulations 2021.

Where an organisation has reason to believe that a data breach has occurred, it must conduct, reasonably and expeditiously, an assessment as to whether the data breach is notifiable. Data intermediaries must notify the organisation for which it is processing personal data on its behalf without undue delay.

Obligation to notify the PDPC

Under Section 26D(1) of the PDPA (read with section 26B of the PDPA), organisations must notify the PDPC as soon as practicable, but, in any case, no later than three calendar days after determining that the data breach is a notifiable data breach.

Obligation to notify affected individuals

Under section 26D(2) of the PDPA, organisations must notify affected individuals if the data breach is likely to result in significant harm or impact to the individuals to whom the information relates. There are two exceptions to this, which are set out under section 26D(5) of the PDPA. Specifically, these exceptions are:

- where organisations have taken actions under any prescribed requirements that render it unlikely that the breach will result in significant harm to affected individuals; and
- where the personal data that was compromised by the data breach is subject to technological protection (eg, encryption) such that the data breach is unlikely to result in significant harm to the affected individuals.

Organisations must also not notify affected individuals if instructed by a prescribed law enforcement agency or directed as such by PDPC (eg, in circumstances where such notification may compromise investigations or prejudice enforcement efforts).

Law stated - 16 May 2024

INTERNAL CONTROLS

Accountability

Are owners or processors of PI required to implement internal controls to ensure that they are responsible and accountable for the PI that they collect and use, and to demonstrate compliance with the law?

Part 3 of the Personal Data Protection Act 2012 (PDPA) sets out the general rules with respect to the protection of and accountability for personal data. These general rules include the following:

- an organisation must develop and implement policies and practices that are necessary for the organisation to meet the obligations of the organisation under the PDPA; and
- an organisation must develop a process to receive and respond to complaints that may arise with respect to the application of the PDPA.

Law stated - 16 May 2024

Data protection officer

Is the appointment of a data protection officer mandatory? What are the data protection officer's legal responsibilities? Are there any criteria that a person must satisfy to act as a data protection officer?

Yes, it is mandatory to appoint a data protection officer (DPO). Pursuant to the accountability obligation under the PDPA, organisations are required to designate one or more individuals to be responsible for ensuring the organisation's compliance with the PDPA (section 11(3) of the PDPA).

This appointed individual (typically known as the DPO) must have the appropriate expertise and knowledge to ensure that the organisation complies with the PDPA and be amply empowered to develop a process to receive and respond to complaints concerning the organisation's compliance with the PDPA.

The Personal Data Protection Commission's (PDPC) Guide to Developing a Data Protection Management Programme (revised 14 September 2021) recommends that the responsibilities of a DPO may include, but are not limited to, the following:

- driving the development and review of data protection policies and processes;
- ensuring compliance with the PDPA through data protection policies and processes;
- fostering a personal data protection culture within the organisation and communicating the organisation's personal data protection policies to stakeholders;
- identifying and alerting management to any risk that might arise with regard to the personal data handled by the organisation;
- handling access and correction requests to personal data;
- managing personal data protection-related queries and complaints; and
- engaging with the PDPC on personal data protection matters, if necessary.

Law stated - 16 May 2024

Record-keeping

Are owners or processors of PI required to maintain any internal records relating to the PI they hold?

Section 12 of the PDPA requires an organisation to develop and implement policies and practices that are necessary for the organisation to meet its obligations under the PDPA and make information about its policies and procedures available on request.

According to the Key Concept Guidelines, organisations should develop both internal and external data protection policies and practices, taking into account the types and amount of personal data they collect and the purposes for such collection.

The PDPC's Guide to Developing a Data Protection Management Programme also recommends that organisations establish a data inventory (among other things). In a 2022 enforcement decision, the PDPC similarly emphasised that an organisation must first know what its personal data assets are, so as to effectively safeguard the personal data in its possession and control; the surest way to ensure such visibility is to maintain a comprehensive personal data asset inventory.

Law stated - 16 May 2024

Risk assessment

Are owners or processors of PI required to carry out a risk assessment in relation to certain uses of PI?

The PDPA expressly requires an organisation to carry out a risk assessment where the organisation intends to collect, use or disclose personal data by relying on either of the following grounds.

Deemed consent by notification

In brief, under section 15A(2) of the PDPA, an organisation may deem that an individual has given consent for a purpose when the individual is notified of the collection, use or disclosure of his or her personal data and how he or she may opt out, but he or she does not opt out within a specified period.

If an organisation intends to rely on this ground, it must conduct an assessment to determine that the proposed collection, use or disclosure of the personal data is not likely to have an adverse effect on the individual per section 15A(4)(a) of the PDPA.

Legitimate interests

In brief, an organisation can collect, use or disclose personal data without consent about an individual if it is in the legitimate interests of the organisation or another person.

If an organisation intends to rely on this ground, it must conduct an assessment to determine that the legitimate interests of the organisation or other person outweigh any adverse effect on the individual. In carrying out the risk assessment, an organisation must:

- identify any adverse effects that the proposed collection, use or disclosure of the personal data for the purpose concerned is likely to have on the individual; and
- identify and implement reasonable measures to:
    - eliminate the adverse effect;
    - reduce the likelihood that the adverse effect will occur; or
    - mitigate the adverse effect.

Law stated - 16 May 2024

Design of PI processing systems

Are there any obligations in relation to how PI processing systems must be designed?

There are no express obligations in the PDPA on how personal information processing systems must be designed, such as requiring privacy-by-design.

However, the PDPC has recommended a data protection-by-design approach in its various guides, for example, its Guide to Developing a Data Protection Management Programme and Guide to Data Protection Practices for ICT Systems.

Law stated - 16 May 2024

REGISTRATION AND NOTIFICATION

Registration

Are PI owners or processors of PI required to register with the supervisory authority? Are there any exemptions? What are the formalities for registration and penalties for failure to do so?

There is no requirement under the Personal Data Protection Act 2012 (PDPA) for organisations that collect, use or disclose personal data (whether in the capacity of a principal organisation or a data intermediary) to register with the Personal Data Protection Commission. However, a data protection officer (DPO) may choose to register with the PDPC to keep abreast of developments in the PDPA.

Law stated - 16 May 2024

Other transparency duties

Are there any other public transparency duties?

While there is no express requirement for an organisation to make public statements on the nature of its processing of personal data per se, organisations are required under the accountability obligation to develop and implement policies and practices that are necessary for the organisation to meet its obligations under the PDPA, and to make such policies and practices available on request (section 12 of the PDPA).

As part of the accountability obligation, an organisation is also required to appoint a DPO and make available his or her business contact information to the public (section 11 of the PDPA). The DPO must have appropriate expertise and knowledge to be able to ensure that the organisation complies with the PDPA, and must develop a process to receive and respond to complaints concerning the organisation's compliance with the PDPA.

Law stated - 16 May 2024

SHARING AND CROSS-BORDER TRANSFERS OF PI

Sharing of PI with processors and service providers

How does the law regulate the sharing of PI with entities that provide outsourced processing services?

Organisations that process personal data on behalf of another organisation (the primary organisation) are considered 'data intermediaries' under the Personal Data Protection Act 2012 (PDPA). The PDPA imposes fewer obligations on the data intermediary where they are processing personal data on behalf of and for the purposes of the primary organisation pursuant to a contract that is evidenced or made in writing.

Data intermediaries are subject only to the data protection provisions relating to the protection and retention of personal data and the duty to notify the primary organisation without undue delay where they have reason to believe that a data breach has occurred concerning personal data that they are processing on the primary organisation's behalf.

Under the PDPA, the primary organisation is deemed to 'have the same obligation under [the PDPA] in respect of personal data processed on its behalf and for its purposes by a data intermediary as if the personal data were processed by the organisation itself'. In this regard, the Personal Data Protection Commission's (PDPC) Guide to Managing Data Intermediaries states that the primary means by which an organisation may ensure appropriate protection of the personal data processed by its data intermediary is through a contract, and that it would be a breach of the PDPA if there is no contractual agreement or document setting out the key obligations and responsibilities of the data intermediary.

Further, the Advisory Guidelines on Key Concepts in the Personal Data Protection Act state that it is important that an organisation is clear as to its rights and obligations when dealing with another organisation and, where appropriate, include provisions in its written contracts to clearly set out each organisation's responsibilities and liabilities in relation to the personal data in question, including whether one organisation is to process personal data on behalf of and for the purposes of the other organisation.

To the extent that the data intermediaries reside overseas or the processing of personal data by such data intermediaries involves the transfer of personal data out of Singapore, the primary organisation would also need to comply with the Transfer Limitation Obligation under section 26 of the PDPA.

Law stated - 16 May 2024

Restrictions on third-party disclosure

Are there any specific restrictions on the sharing of PI with recipients that are not processors or service providers?

An organisation's disclosure of an individual's personal data to other recipients must be made following the applicable requirements under the PDPA. In other words, if an organisation wishes to disclose an individual's personal data to a third-party recipient, the organisation must first obtain valid consent from the individual him or herself, which includes providing notification of the specified purposes for which the organisation intends to disclose the individual's personal data, unless an exception applies.

Where the disclosure is to a third-party recipient that is outside of Singapore, the organisation must also ensure that it complies with the applicable cross-border data transfer requirements.

Law stated - 16 May 2024

Cross-border transfer

Is the transfer of PI outside the jurisdiction restricted?

Yes, section 26 of the PDPA requires organisations transferring personal data overseas to do so only in accordance with the requirements prescribed under the PDPA to ensure that the recipients provide the transferred personal data a standard of protection that is comparable to the PDPA.

In particular, under the Personal Data Protection Regulations 2021 (PDP Regulations), the transferring organisation must, before transferring the personal data outside of Singapore, take appropriate steps to ascertain whether, and to ensure that, the recipient is bound by legally enforceable obligations to provide the transferred personal data with a standard of protection comparable to that under the PDPA.

'Legally enforceable obligations' is defined in the PDP Regulations 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 (in cases where a recipient is an organisation related to the transferring organisation) 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 binding corporate rules apply,
- the countries and territories to which the personal data may be transferred under the binding corporate rules, and
- the rights and obligations provided by the binding corporate rules; or
- any other legally binding instrument.

In relation to binding corporate rules, the PDP Regulations define a recipient as being related to the transferring organisation if:

- the recipient, directly or indirectly, controls the transferring organisation;
- the recipient is, directly or indirectly, controlled by the transferring organisation; or
- the recipient and the transferring organisation are, directly or indirectly, under the control of a common person.

For completeness, the PDP Regulations provide for certain prescribed situations whereby the transfer limitation obligation is taken to be satisfied and it is not necessary to impose legal enforcement obligations (eg, where the personal data is publicly available in Singapore or where the personal data is data in transit).

The PDP Regulations also recognise the certification systems under the Asia-Pacific Economic Cooperation (APEC) Cross-Border Privacy Rules (CBPR) System and the Privacy Recognition for Processors (PRP) System as one of the modes for the transfers of data overseas. If the recipient holds a specified certification (ie, certification under the APEC CBPR or PRP) that is granted or recognised under the law of that country or territory to which the personal data is transferred, the recipient is taken to be bound by legally enforceable obligations to provide a standard of protection for the transferred personal data that is at least comparable to the protection under the PDPA.

Law stated - 16 May 2024

Further transfer

If transfers outside the jurisdiction are subject to restriction or authorisation, do these apply equally to transfers to service providers and onwards transfers?

The Key Concept Guidelines provide that where an organisation engages a data intermediary to process personal data on its behalf and for its purposes, the organisation continues to be responsible for complying with all data protection obligations under the PDPA as if the personal data were processed by the organisation itself. This would include the transfer limitation obligation, where the local data intermediary transfers personal data overseas, as part of its processing for and on the organisation's behalf.

For onward transfers of personal data (ie, subsequent transfers by the overseas recipient to another party), the PDPA does not expressly impose the transfer limitation obligation on the overseas recipient. However, the Association of Southeast Asian Nations (ASEAN) Model Contractual Clauses for Cross-Border Data Flows (ASEAN MCCs) includes the following clause, 'The Data Importer agrees that prior to any disclosure or transfer of Personal Data to third parties, including Data Processors, the Data Importer shall ensure that the third party shall be subject to and bound by the obligations of the Data Importer to the Data Exporter.' The PDPC encourages the use of these ASEAN MCCs, and has also issued guidance that states that these ASEAN MCCs set out baseline responsibilities of the data exporter and data importer.

Separately, the PDP Regulations provide an exemption for 'data in transit', which, in summary, refers to personal data transferred through Singapore in the course of onward transportation to a country or territory outside Singapore, without the personal data being accessed or used by, or disclosed to, any organisation while the personal data is in Singapore, except for the purpose of such transportation. An overseas organisation transferring personal data through Singapore to an overseas destination will be deemed to comply with the transfer limitation obligation in respect of such data in transit.

Law stated - 16 May 2024

Localisation

Does the law require PI or a copy of PI to be retained in your jurisdiction, notwithstanding that it is transferred or accessed from outside the jurisdiction?

There is no express requirement under the PDPA that requires personal information (PI) or a copy of PI to be retained in the jurisdiction, notwithstanding that it is transferred or accessed from outside the jurisdiction.

Law stated - 16 May 2024

RIGHTS OF INDIVIDUALS

Access

Do individuals have the right to access their personal information held by PI owners? Describe how this right can be exercised as well as any limitations to this right.

Yes, under section 21 of the Personal Data Protection Act 2012 (PDPA), individuals have the right to request an organisation to provide them with their personal data that is in the possession or under the control of the organisation, and information about how that personal data has been or may have been used or disclosed within a year before the date of the access request.

This individual's right of access is not an unfettered one. There are several exceptions as set out in section 21(3) of the PDPA. Organisations are not allowed to provide an individual with his or her personal data or other information where such provision 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 his or her identity; or
- be contrary to the national interest.

Concerning exceptions in bullet points three and four, these two exceptions would not apply to any user activity data about, or any user-provided data from the requesting individual, despite such data containing third-party personal data.

Further, the Fifth Schedule to the PDPA sets out certain situations where organisations are not required to accede to such requests, for example, concerning:

- opinion data kept solely for an evaluative purpose;
- documents relating to a prosecution, if all proceedings related to the prosecution have not been completed;
- personal data that is subject to legal privilege;
- personal data that, if disclosed, would reveal confidential commercial information that could, in the opinion of a reasonable person, harm the competitive position of the organisation;
- 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; or
- any request:
    - that would unreasonably interfere with the operations of the organisation because of the repetitious or systematic nature of the requests;

- if the burden or expense of providing access would be unreasonable to the organisation or disproportionate to the individual's interests;
- for information that does not exist or cannot be found;
- for trivial information; or
- that is otherwise frivolous or vexatious.

Under the Personal Data Protection Regulations 2021 (the PDP Regulations), organisations are entitled to charge the individual a reasonable fee for access to his or her personal data, provided that the organisation gives the individual a written estimate of the fee. This is to allow organisations to recover the incremental costs incurred in the form of time and effort spent by the organisation in responding to the access request. If an individual is not satisfied with the fee that is being charged by the organisation, the individual may, under section 48H(1)(d) of the PDPA, make an application to the Personal Data Protection Commission (PDPC) for the PDPC to review the fee. The PDPC may, upon completion of its review, confirm, reduce or disallow a fee, or direct the organisation to make a refund to the complainant or receiving organisation (as the case may be).

Organisations are required to respond to an access request as soon as reasonably possible. Subject to this, the PDP Regulations provide that, if an organisation is unable to respond to an access request within 30 days from the request, it must inform the individual in writing within that same time frame of the time by which it will be able to respond to the request (which should be the soonest possible time when it can provide access).

If an organisation does not accede to an individual's request to provide that individual access to his or her personal data, the individual may make an application to the PDPC to review the organisation's refusal to provide access to personal data requested by the individual, or a failure to provide such access within a reasonable time under section 48H(1)(a) of the PDPA. Upon completion of its review, the PDPC may confirm the refusal to provide access to the personal data or direct the organisation to provide access to the personal data, within such time as the PDPC may specify.

Additionally, organisations must also preserve a copy of the personal data requested pursuant to an access request for 30 days after the rejection of the request or until the individual has exhausted the right to apply for a reconsideration or appeal, whichever is later.

Law stated - 16 May 2024

Other rights
Do individuals have other substantive rights?

Correction obligation

Yes, section 22 of the PDPA provides an individual with the right to request an organisation to correct any error or omission in his or her personal data that is in the possession of or under the control of the organisation. This is, however, subject to the exceptions listed in the Sixth Schedule to the PDPA (eg, if the request relates to opinion data kept solely by the organisation for an evaluative purpose). Notably, the Sixth Schedule to the PDPA excludes

'derived personal data' from the application of the correction obligation. 'Derived personal data':

- means personal data about an individual that is derived by an organisation in the course of business from other personal data, about the individual or another individual, in the possession or under the control of the organisation; but
- does not include personal data derived by the organisation using any prescribed means or method.

Organisations are required to correct the personal data as soon as reasonably practicable. Subject to this, the PDP Regulations provide that if an organisation is unable to make the necessary correction within 30 days from the request, it is required to inform the individual in writing within the same time frame of the time by which it will be able to do so (which should be the soonest practicable time when it can correct).

Unless it is satisfied on reasonable grounds that a correction should not be made, an organisation is required to correct the personal data and send the corrected personal data to every organisation to which the personal data was disclosed within one year of the date the amendment was made, insofar as that organisation needs the corrected personal data for any legal or business purpose.

Unlike access requests, organisations are not entitled to charge a fee for correction requests.

Withdrawal of consent

An individual may, at any time, withdraw any consent given or deemed to have been given under the PDPA in respect of the collection, use or disclosure of their personal data for any purpose by an organisation (section 16 of the PDPA). Organisations must not prohibit an individual from withdrawing consent and should not have inflexible consent withdrawal policies.

Several requirements must be complied with by either the individual or the organisation concerning a withdrawal of consent:

- the individual must give reasonable notice of the withdrawal to the organisation;
- on receipt of the notice, the organisation must inform the individual of the consequences of withdrawing consent;
- an organisation must not prohibit an individual from withdrawing consent, although this does not affect any legal consequences arising from such withdrawal; and
- upon withdrawal of consent, the organisation must cease (and cause its data intermediaries and agents to cease) collecting, using or disclosing the personal data, as the case may be, unless the collection, use or disclosure of the personal data without consent is required or authorised under the PDPA or any other written law.

Data portability obligation

Under the Personal Data Protection (Amendment) Act 2020 (the Amendment Act), a new data portability obligation will be introduced. While the provisions relating to data portability (ie, Part 6B of the PDPA) have been passed, the provisions will only come into effect at a later date, together with the issuance of regulations. It is anticipated that these regulations will prescribe further details such as:

- the data categories to which the obligation applies; and
- the technical and process details for the transmission.

Law stated - 16 May 2024

Compensation

Are individuals entitled to monetary damages or compensation if they are affected by breaches of the law? Is actual damage required or is injury to feelings sufficient?

Yes, under section 480 of the PDPA, any person who suffers loss or damage directly as a result of non-compliance by an organisation with any provision in Parts 4 to 6B, or by a person with any provision in Division 3 of Part 9 or section 48B(1) of the PDPA will have a right of action for relief in civil proceedings in a court. The court may grant a claimant any relief as it thinks fit, including the award of an injunction or declaration, or damages.

However, where the PDPC has issued a decision under the PDPA in respect of such contravention, this right of private action is only exercisable after the PDPC's decision has become final (as a result of there being no further right of appeal).

Law stated - 16 May 2024

Enforcement

Are these rights exercisable through the judicial system or enforced by the supervisory authority or both?

Where the PDPC is satisfied that an organisation has breached the data protection provisions under the PDPA, the PDPC is empowered with wide discretion to issue such remedial directions as it thinks fit, including the imposition of a financial penalty that does not exceed S$1 million, or 10 per cent of the organisation's annual gross turnover in Singapore, whichever is higher.

Should any organisation or individual be aggrieved by the PDPC's decision or direction, such organisation or individual may request the PDPC to reconsider its decision or direction. Thereafter, any organisation or individual aggrieved by the PDPC's reconsideration decision may submit an appeal to the Data Protection Appeal Panel. Alternatively, an aggrieved organisation or individual may appeal directly to the Data Protection Appeal Panel without first submitting a reconsideration request.

An appeal can be made against the Data Protection Appeal Panel's decision to the High Court on limited grounds, namely on a point of law or as to the amount of a financial penalty.

Reconsideration applications and appeal requests must be made within 28 days after the issuance of the relevant direction or decision; there is no automatic suspension of the direction or decision concerned except in the case of the imposition of a financial penalty or the amount thereof.

Separately, an individual has the right to commence a private action (ie, civil proceedings) for loss or damage suffered directly as a result of an organisation's non-compliance with the PDPA.

Law stated - 16 May 2024

EXEMPTIONS, DEROGATIONS AND RESTRICTIONS

Further exemptions and restrictions

Does the law include any derogations, exclusions or limitations other than those already described?

Business contact information

The application of the data protection provisions does not extend to 'business contact information', (unless expressly referred to), which is defined as 'an individual's name, position name or title, business telephone number, business address, business electronic mail address or business fax number and other similar information about the individual, not provided by the individual solely for his or her personal purposes'.

Exclusions from DNC provisions

As regards the Do Not Call (DNC) provisions, certain messages are excluded from the meaning of a specified message under the Eighth Schedule to the Personal Data Protection Act 2012 and therefore not subject to the application of the DNC provisions. Such exceptions include the following:

- any message sent by a public agency under, or to promote, any programme carried out by any public agency that is not for a commercial purpose;
- any message sent by an individual acting in a personal or domestic capacity;
- any message that is necessary to respond to an emergency that threatens the life, health or safety of any individual;
- any message the sole purpose of which is:
    - to facilitate, complete or confirm a transaction that the recipient has previously agreed to enter into with the sender;
    - to provide warranty information, product recall information or safety or security information concerning a product or service purchased or used by the recipient; or
    -

to deliver goods or services, including product updates or upgrades, that the recipient is entitled to receive under the terms of a transaction that the recipient has previously agreed to enter into with the sender;

- any message (other than a message set out in the point directly above):
  - that is sent while the sender is in an ongoing relationship with the recipient of the message; and
  - the sole purpose of which relates to the subject matter of the ongoing relationship. An 'ongoing relationship' means a relationship, on an ongoing basis, between the sender and the recipient of the message, arising from the carrying on or conduct of a business or an activity (commercial or otherwise) by the sender;
- any message the sole purpose of which is to conduct market research or market survey; and
- any message sent to an organisation other than an individual acting in a personal or domestic capacity, for any purpose of the receiving organisation.

Law stated - 16 May 2024

SPECIFIC DATA PROCESSING

Cookies and similar technology

Are there any rules on the use of 'cookies' or equivalent technology?

The Personal Data Protection Commission (PDPC) has noted that any personal data collected through the use of cookies would not be treated differently from other types of personal data, and organisations that collect personal data using cookies would equally be subject to the requirements of the PDPA. Organisations are only required to obtain consent for cookies that collect personal data. Organisations do not need to obtain consent for cookies that do not collect personal data (eg, session cookies may only collect and store technical data needed to play back a video on a website).

The Selected Topics Guidelines clarify that there may not be a need to seek consent for the use of cookies to collect, use or disclose personal data for Internet activities that the user has clearly requested, where the individual is aware of the purposes for such collection, use or disclosure and voluntarily provides his or her personal data for such purposes. Such activities include transmitting personal data for effecting online communications and storing information that the user enters in a web form to facilitate an online purchase.

Further, for activities that cannot take place without cookies that collect, use or disclose personal data, consent may be deemed to have been given if the individual voluntarily provides the personal data for that purpose of the activity, and it is reasonable that he or she would do so.

In situations where the individual configures his or her browser to accept certain cookies but rejects others, he or she may be deemed to have consented to the collection, use and disclosure of the personal data by the cookies that he or she has chosen to accept. However, the mere failure of an individual to actively manage his or her browser settings does not

imply that he or she has consented to the collection, use and disclosure of personal data by all websites for their stated purpose.

Also, the Selected Topics Guidelines make clear that where organisations use cookies for personalised advertisement targeting that involves the collection and use of an individual's personal data, the individual's consent is required.

Law stated - 16 May 2024

Electronic communications marketing

Are there any rules on marketing by email, fax, telephone or other electronic channels?

Organisations that make telemarketing calls or send messages of a commercial nature (which are considered to be 'specified messages' under the Do Not Call (DNC) provisions) are required to obtain valid confirmation that the Singapore telephone number is not listed in the DNC Registry within 21 days before sending the specified message. This may be done by:

- making an application to confirm whether the Singapore telephone number is listed in the DNC Registry; or
- obtaining information from third-party checks that the Singapore telephone number is not listed in the DNC Registry.

Organisations may also wish to refer to the PDPC's Advisory Guidelines on Requiring Consent for Marketing Purposes.

Regarding the rules on marketing emails, the Spam Control Act governs the sending of unsolicited electronic communications in bulk in Singapore.

In general, under the Spam Control Act, any person who sends, causes to be sent or authorises the sending of unsolicited commercial electronic messages in bulk, is required to include within the message:

- an unsubscribe facility for the recipient to unsubscribe from such messages;
- where there is a subject field, a title in the subject field, which is not false or misleading as to the content of the message;

the letters '' with a space before the title in the subject field, or if there is no subject field, in the words first appearing in the message, to clearly identify that the message is an advertisement;

- header information that is not false or misleading; and
- an accurate and functional electronic mail address or telephone number by which the sender can be readily contacted.

Law stated - 16 May 2024

Targeted advertising

Are there any rules on targeted online advertising?

There are no specific rules relating to targeted online advertising under the PDPA. However, the PDPA's general data protection obligations would apply if there is any collection, use or disclosure of personal data for such purpose (such as the obligation to obtain consent, unless an exception applies under the PDPA).

Law stated - 16 May 2024

Sensitive personal information

Are there any rules on the processing of 'sensitive' categories of personal information?

The PDPA does not have specific rules relating to the processing of 'sensitive' categories of personal information. However, as a number of the data protection provisions adopt a standard of reasonableness, the sensitivity of the personal data in question could, in practice, affect the measures that an organisation must put in place to ensure compliance. For instance, section 24 of the PDPA requires that an organisation make 'reasonable security arrangements' to protect personal data in its possession or under its control, to prevent:

- unauthorised 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.

The PDPC has noted that organisations should take into account the sensitivity of personal data when deciding on the appropriate level of security arrangements needed to protect it.

Notably, the PDPC also imposes more stringent guidelines concerning National Registration Identity Card (NRIC) numbers and other national identification numbers. According to the Advisory Guidelines on the PDPA for NRIC and other National Identification Numbers (issued on 31 August 2018), organisations are generally not allowed to collect, use or disclose NRIC numbers and other national identification numbers unless such collection, use or disclosure is required under the law (or an exception under the PDPA applies), or is necessary to accurately establish or verify the identity of the individual to a high degree of fidelity.

Law stated - 16 May 2024

Profiling

Are there any rules regarding individual profiling?

There are no specific rules relating to profiling under the PDPA. However, the PDPA's data protection obligations would apply if there is any collection, use or disclosure of personal data for such purpose (eg, the obligation to obtain consent, unless an exception applies under the PDPA).

Law stated - 16 May 2024

Cloud services

Are there any rules or regulator guidance on the use of cloud computing services?

The PDPC's Guide to Data Protection Practices for ICT Systems provides guidance for organisations that use cloud service providers (CSPs). For instance, organisations that adopt cloud services for the management of personal data need to be aware of the security and compliance challenges that are unique to cloud services, and where the CSP is unable to customise a service for the organisation, the organisation must decide if the security measures put in place by the CSP provides reasonable security for the personal data.

CSPs are required to comply with the PDPA (in particular, the obligation to implement reasonable security arrangements to protect personal data in their possession or under their control), any applicable subsidiary legislation that may be enacted from time to time, and any applicable sector-specific data protection frameworks to the extent that CSPs provide cloud services to customers operating in these sectors.

Notably, CSPs are required to make reasonable security arrangements to protect personal data in their possession or under their control. The Selected Topics Guidelines state that industry standards such as the ISO 27001 and Tier 3 of the Multi-Tiered Cloud Security Certification Scheme could provide assurance of the CSP's ability to comply with the protection obligation. Additionally, the PDPC has stated in its Selected Topics Guidelines that when engaging CSPs, organisations should ensure that any overseas transfer of personal data will be done following the requirements under the PDPA, namely, that the organisation should ensure that the CSP only transfers data to locations with comparable data protection regimes, or has legally enforceable obligations to ensure a comparable standard of protection for the transferred personal data. This is regardless of whether the CSP is located in Singapore or overseas. The organisation may be considered to have taken appropriate measures to comply with the transfer limitation obligation by ensuring that personal data may only be transferred to overseas locations with comparable data protection laws, or that the recipients (eg, data centres or sub-processors) in these locations are legally bound by similar contractual standards.

Law stated - 16 May 2024

UPDATE AND TRENDS

Key developments of the past year

Are there any emerging trends or hot topics in international data protection in your jurisdiction?

Emerging trends and hot topics include the protection of children's personal data and artificial intelligence (AI).

Recently, the Personal Data Protection Commission (PDPC) published its Advisory Guidelines on the PDPA for Children's Personal Data in the Digital Environment (Children's Personal Data Guidelines) to provide guidance to organisations as to how the data protection provisions in the Personal Data Protection Act 2012 (PDPA) apply to children's personal data in the digital environment. For instance, the Children's Personal Data Guidelines clarify that

a child aged between 13 and 17 may give valid consent when the policies on the collection, use and disclosure of the child's personal data as well as the withdrawal of consent, are readily understandable by them. Additionally, the use of a child's personal data or profile to target harmful or inappropriate content (as defined in the Code of Practice for Online Safety (Online Safety Code), issued under the Broadcasting Act 1994 (Broadcasting Act)) would be an unreasonable purpose. The PDPC also advises organisations to conduct data protection impact assessments before releasing products or services that are likely to be accessed by children to meet their accountability obligation under the PDPA.

In line with the objective of ensuring children's safety online, the Online Safety (Miscellaneous Amendments) Act was passed on 24 November 2022 and took effect on 1 February 2023. As a result, a new Part 10A was introduced to the Broadcasting Act, among other things. Part 10A empowers the Info-communications Media Development Authority (IMDA) to designate social media services with significant reach or impact in Singapore to comply with the Online Safety Code, and issue directions to online communication services providers and internet access service providers regarding specified egregious content. The Online Safety Code, which took effect on 18 July 2023, requires designated social media services (Facebook, HardwareZone, Instagram, TikTok, X, and YouTube) to put in place additional safeguards for children.

In relation to AI, we anticipate that organisations will be increasingly concerned about ensuring that their AI-powered technologies comply with the PDPA. In this regard, on 1 March 2024, the PDPC issued the Advisory Guidelines on the Use of Personal Data in AI Recommendation and Decision Systems. The PDPC provided guidance on how the PDPA applies to three key stages of AI system implementation: development, deployment and procurement.

The IMDA has also developed several tools to help organisations use AI and data responsibly. Notably, it has released a second edition of its Model AI Governance Framework in 2020, which aims to assist organisations to demonstrate reasonable effort to align their policies with relevant accountability-based practices in data protection (eg, the PDPA and the OECD Privacy Principles). The IMDA is expected to issue a new Model AI Governance Framework for Generative AI that expands on the existing framework in mid-2024.

Law stated - 16 May 2024