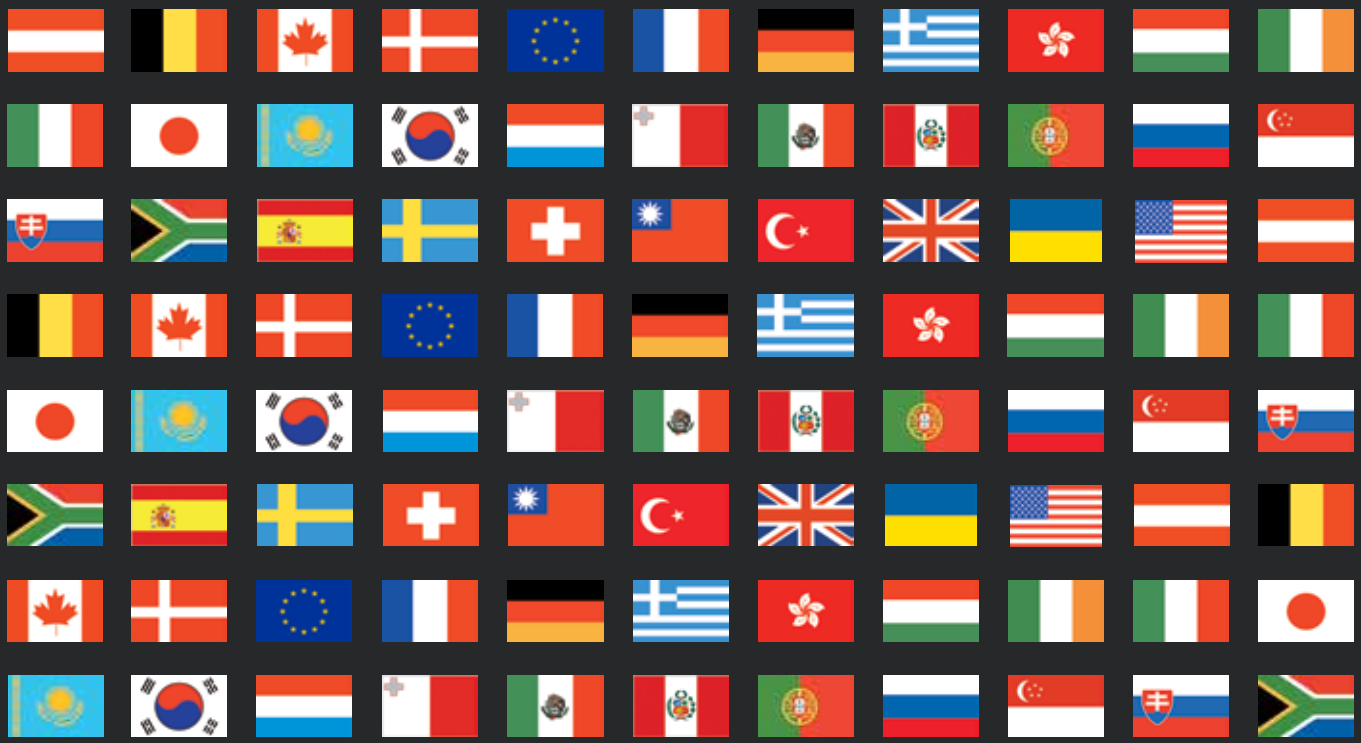
Data Protection & Privacy

In 31 jurisdictions worldwide

Contributing editor
Rosemary P Jay



2015

GETTING THE DEAL THROUGH

GETTING THE DEAL THROUGH

Data Protection & Privacy 2015

Contributing editor

Rosemary P Jay

Hunton & Williams

Publisher
Gideon Roberton
gideon.roberton@lbresearch.com

Subscriptions
Sophie Pallier
subscriptions@gettingthedealthrough.com

Business development managers
George Ingledew
george.ingledew@lbresearch.com

Alan Lee
alan.lee@lbresearch.com

Dan White
dan.white@lbresearch.com

Law Business Research

THE QUEEN'S AWARDS FOR ENTERPRISE: 2012

Published by
Law Business Research Ltd
87 Lancaster Road
London, W11 1QQ, UK
Tel: +44 20 7908 1188
Fax: +44 20 7229 6910

First published 2012
Third edition
ISSN 2051-1280

Printed and distributed by
Encompass Print Solutions
Tel: 0844 2480 112

CONTENTS

Singapore

Lim Chong Kin and Charmian Aw
Drew & Napier LLC

Law and the regulatory authority

1 Legislative framework

Summarise the legislative framework for the protection of personally identifiable information (PII). Does your jurisdiction have a dedicated data protection law? Have any international instruments on privacy or data protection been adopted in your jurisdiction?

Prior to the enactment of the Personal Data Protection Act 2012 (No. 26 of 2012) (PDPA), Singapore did not have an overarching law governing the protection of personally identifiable information. The collection, use and disclosure of personal data in Singapore were regulated to a certain extent by a patchwork of laws including common law, sector-specific legislation and various self-regulatory or co-regulatory codes. These existing sector-specific data protection frameworks will continue to operate alongside the PDPA.

The PDPA was implemented in three phases. On 2 January 2013, selected provisions of the PDPA came into operation. These include provisions that:

- set out the scope and interpretation of the PDPA;
- provide for the establishment of the Personal Data Protection Commission (PDPC) and the Data Protection Advisory Committee; and
- provide for the establishment of Do-Not-Call (DNC) registers by the PDPC, and other general provisions of the PDPA.

On 2 January 2014, provisions relating to the DNC Registry came into force; and the main data protection provisions under the PDPA came into effect on 2 July 2014.

Regulations and advisory guidelines under the PDPA deal with specific issues in greater detail.

The Personal Data Protection Regulations 2014 (PDP Regulations) were gazetted on 19 May 2014. The PDP Regulations supplement the PDPA in three key areas as follows:

- the requirements for transfers of personal data out of Singapore;
- 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 in relation to disclosure of personal data of deceased individuals.

In addition, the PDPC has issued a number of advisory guidelines to provide greater clarity on the interpretation of the PDPA, namely:

- Advisory Guidelines on Key Concepts in the Personal Data Protection Act (Key Concepts Guidelines);
- Advisory Guidelines on the Personal Data Protection Act for Selected Topics (Selected Topics Guidelines);
- Advisory Guidelines on the Do Not Call Provisions;
- Advisory Guidelines for the Telecommunication Sector; and
- Advisory Guidelines for the Real Estate Agency Sector.

In addition, the following set of proposed guidelines was issued on 16 May 2014 for public consultation:

- Proposed Advisory Guidelines for the Education Sector;
- Proposed Advisory Guidelines for the Healthcare Sector;
- Proposed Advisory Guidelines for the Social Service Sector; and
- Proposed Advisory Guidelines on the PDPA for Selected Topics – Photography.

While Singapore has not formally adopted international instruments on privacy or data protection, 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, the then Ministry 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 OECD Guidelines on the Protection of Privacy and Transborder Flow of Personal Data and the APEC Privacy Framework, in developing the PDPA framework.

2 Data protection authority

Which authority is responsible for overseeing the data protection law? Describe the powers of the authority.

The PDPA is administered and enforced by the PDPC. The PDPC was established as a statutory body under the PDPA on 2 January 2013 and is under the purview of the Ministry of Communications and Information (MCI). The members of the PDPC are appointed by the MCI and the PDPC is currently chaired by Mr Leong Keng Thai, who is also the deputy chief executive and director-general (telecoms and post) of the Infocomm Development Authority of Singapore (IDA). Under him are four other members, namely:

- Ms Aileen Chia, assistant chief executive and deputy director-general (telecoms and post), IDA;
- Mr Ong Tong San, director (competition and market access), IDA;
- Mr Amos Tan, director (strategy and innovation), IDA; and
- Ms Koh Li-Na, assistant chief executive, Early Childhood Development Agency.

In the course of its investigation, the PDPC may:

- by notice in writing, require an organisation to produce any specified document or specified information;
- by giving at least two working days' advance notice of intended entry, enter an organisation's premises without a warrant; and
- obtain a search warrant to enter an organisation's premises and take possession of, or remove, any document.

The PDPC is also empowered to:

- refer complaints to mediation with mutual consent of the complainant and the organisation involved;
- review complaints;
- issue directions to an offending organisation to stop collecting, using or disclosing personal data, or to destroy personal data collected in breach of the PDPA; and
- impose financial penalties of up to S$1 million.

The PDPA also establishes the Data Protection Advisory Committee, which advises the PDPC on matters relating to the review and administration of the personal data protection framework. Currently, the eight-man Advisory Committee is headed by Ms Liew Woon Yin, director of Abundanti and former director-general of the Intellectual Property Office of Singapore.

3 Breaches of data protection

Can breaches of data protection lead to criminal penalties? How would such breaches be handled?

Generally, individuals affected by an organisation's non-compliance with the main data protection provisions have a right to seek remedies. The main data protection provisions are found under parts III to VI of the PDPA, and set out the obligations of organisations with respect to the collection, use, disclosure, access to, correction, and care of personal data.

Any individual may lodge a complaint with the PDPC in respect of non-compliance by an organisation with any of the provisions under parts III to VI of the PDPA. Upon receipt of a complaint, the PDPC may exercise a range of enforcement powers. According to public guidance published on the PDPC's website as of July 2014, when a complaint is received by the PDPC, the PDPC may assess if it can help to address the individual's concerns by facilitating communications between the individual and organisation. If an individual and an organisation are unable to resolve the matter directly and require additional assistance, the PDPC may refer the matter for mediation by a qualified mediator where both the complainant and the organisation involved have consented to the same. Furthermore, as mentioned (see question 2), the PDPC is empowered to issue directions to an offending organisation to stop collecting, using or disclosing personal data, or to destroy personal data collected in breach of the PDPA, and impose financial penalties of up to S$1 million. In calculating a financial penalty, the PDPC may consider any applicable aggravating or mitigating factors.

Any person who suffers loss or damage directly as a result of a contravention of any of the provisions under parts IV to VI of the PDPA may also commence a private civil action in respect of such loss or damage suffered.

Non-compliance with certain provisions under the PDPA may also constitute an offence, for which a fine or a term of imprisonment may be imposed. The quantum of the fine and the length of imprisonment (if any) vary, depending on which provisions are breached. For instance, a person found guilty of making requests to obtain access to or to correct the personal data of another without authority may be liable on conviction to a fine not exceeding S$5,000 or to imprisonment for a term not exceeding 12 months, or both. The obstruction of PDPC officers (for instance, in the course of their investigations) or provision of false statements to the PDPC may be punishable upon conviction with, in the case of an individual, a fine of up to S$10,000 or imprisonment for a term not exceeding 12 months; and in the case of an organisation, a fine of up to S$100,000. Please refer to question 40 for more circumstances under which criminal sanctions may be imposed under the PDPA.

Scope

4 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 PDPA applies to all 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.

Certain categories of 'organisations' are carved out of the application of the PDPA, such as:

- individuals acting in a personal or domestic capacity;
- employees acting in the course of their employment with an organisation; and
- public agencies, or organisations acting on behalf of a public agency in relation to the collection, use or disclosure of personal data.

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. The PDPA provides that the new general data protection framework 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. For example, the banking secrecy laws under the Banking Act still govern customer information obtained by a bank and the Telecom Competition Code still governs end-user service information obtained by a telecoms licensee.

The PDPC has also published advisory guidelines to address the unique circumstances faced by organisations in the telecommunication and real estate sectors in complying with the PDPA. A number of other proposed sector-specific guidelines have also been issued for public consultation (see question 1).

5 Communications, marketing and surveillance laws

Does the data protection law cover interception of communications, electronic marketing or monitoring and surveillance of individuals? If not, list other relevant laws in this regard.

Interception of communications and monitoring and surveillance of individuals

To the extent that personal data is collected in the interception of communications and in the monitoring and surveillance of individuals, the PDPA applies to the organisation collecting such data. As such, the individual's consent has to be sought before any such collection takes place, unless such consent is not required (see question 10 for more information on the consent requirement and its exceptions).

For example, the Selected Topics Guidelines indicate that an employer may not need to seek consent for any personal data collected from its monitoring employees' use of company computer network resources as long as such collection is reasonable for the purpose of managing or terminating the employment relationship, although under section 20(4) of the PDPA, it is still required to notify its employees of this purpose for such collection of their personal data.

In relation to CCTV surveillance, the Selected Topics Guidelines explicitly clarify that organisations which install CCTVs in their premises are required to put up notices informing individuals that CCTVs are operating in the premises and stating the use and purpose of such surveillance, to fulfil their obligation to obtain consent for the collection, use or disclosure of personal data from CCTV footage. This is unless such consent is not required, for example, if the CCTV surveillance is necessary for any investigation or proceedings, insofar as it is reasonable to expect that seeking the consent of the individual would compromise the availability or the accuracy of the personal data. Moreover, the PDPC recommends that, while such notices should be placed at points of entry or prominent locations in a venue or a vehicle, to enable individuals to have sufficient awareness that CCTV has been deployed in the general locale, they do not have to reveal the exact location of the CCTV cameras. The PDPC also clarifies that an individual may request access to CCTV footage containing his or her image in accordance with the PDPA, unless an exception to this right applies (see question 34 for more details on an individual's right to access his or her personal data and its limitations). However, the PDPC has also indicated that organisations are generally required to provide access to CCTV footage where the images of other individuals present in the CCTV footage are masked as required (assuming that consent from the other individuals for the disclosure of their personal data has not been obtained).

In addition, where the organisations collecting such personal data via the interception of communications and/or the performance of surveillance or monitoring activities are public agencies (eg, the Singapore Police Force or the IDA), they are excluded from the application of the PDPA under section 4(1)(c).Thus, to the extent that the above exceptions apply, the organisation collecting personal data via interception of communication or monitoring and surveillance of individuals will not have to seek the individuals' consent prior to such collection.

Apart from the PDPA, there are other regulations that allow for the interception of communications and the monitoring and surveillance of individuals. Below is a non-exhaustive list of such regulations:

- Organisations providing telecommunications services and holding service-based operation licences may have to comply with interception requests by the IDA and other authorities. Specifically, condition 16 of the IDA's standard SBO (I) licence conditions expressly permit disclosure of subscriber information 'where disclosure of subscriber information is deemed necessary by [the] IDA or such other relevant law enforcement or security agencies in order to carry out their respective functions or duties'. Condition 26.1 of the IDA's standard SBO (I) licence conditions also require licensees to 'provide [the] IDA with any document and information within its knowledge, custody or control, which [the] IDA may, by notice or direction require'.
- Section 15A of the Computer Misuse and Cybersecurity Act states that the minister may authorise or direct any person or organisation to, inter alia, 'provid[e] to the minister or a public officer authorised by him any information (including real-time information) obtained from any computer'.

- Section 20 of the Criminal Procedure Code empowers the police to require the production of a 'document or other thing' (that is necessary for the police investigation) 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 states that the Public Prosecutor may authorise any police officer to, inter alia, 'intercept any message transmitted or received by telecommunication' or 'intercept or listen to any conversation by telephone'.

Electronic marketing

Section 11 of the Spam Control Act requires any person who 'sends, causes to be sent or authorises the sending of unsolicited commercial electronic messages (which include both e-mails and SMS/MMS) in bulk' to comply with certain obligations. These include requirements that unsolicited commercial electronic messages must contain an unsubscribe facility; the label '<ADV>' 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).

In addition to the requirements under the Spam Control Act regarding the sending of spam messages, the PDPA would also apply to personal data collected, used or disclosed through the use of such electronic marketing. Generally, the PDPA requires organisations to obtain consent for a stated purpose to collect, use or disclose the contact information of individuals, unless any exception applies.

6 Other laws

Identify any further laws or regulations that provide specific data protection rules for related areas.

Various other legislation in Singapore sets out specific data protection rules, some of which are sector-specific. For instance:

- the Banking Act proscribes the disclosure of customer information by a bank or its officers;
- the Computer Misuse and Cybersecurity Act deals with computer system hackers and other similar forms of unauthorised access or modification to computer systems;
- the Electronic Transactions Act provides for the security and use of electronic transactions by criminalising any disclosure of electronic data obtained pursuant to the Act, unless the disclosure is expressly allowed under the Act, required by any written law, or mandated by an order of court;
- the Private Hospitals and Medical Clinics Act contains provisions relating to the confidentiality of information held by private hospitals, medical clinics, clinical laboratories and health-care establishments licensed under the Act;
- the Official Secrets Act contains provisions relating to the prevention of disclosure of official documents and information;
- the Statutory Bodies and Government Companies (Protection of Secrecy) Act details provisions concerning protecting the secrecy of information of statutory bodies and government companies; and
- the Telecom Competition Code issued under the Telecommunications Act contains certain provisions pertaining to the safeguarding of end-user service information. Notably, IDA has introduced amendments to the provisions governing end-user service information in the Telecom Competition Code effective 2 July 2014, taking into account that the PDPA will be the primary legislation governing personal data.

On 2 June 2014, the Monetary Authority of Singapore (MAS) also issued its Consultation Paper on the Obligations of Financial Institutions under the Personal Data Protection 2012 – Amendments to AML/CFT Notices, which set out its proposed amendments to the MAS Notices on Prevention of Money Laundering and Countering the Financing of Terrorism (AML/CFT). The proposed amendments sought to clarify financial institutions' (FIs') obligations under the AML/CFT requirements in relation to the PDPA. Accordingly, these proposed amendments were incorporated into notices issued by MAS, pertaining to different classes of FIs, which took effect on 1 July 2014. These amendments apply to the following classes of FIs:

- holders of stored value facilities;
- trust companies;
- approved trustees;
- capital market intermediaries;
- financial advisers;
- life insurers;
- holders of money-changer's licences and remittance licences;
- finance companies;
- merchant banks; and
- commercial banks.

Broadly, they make clear that FIs may continue the existing practice of collecting, using and disclosing personal data without customer consent for the purposes of meeting the AML/CFT requirements, and acknowledge customers' rights under the PDPA to access and correct their personal data that is in the possession or under the control of the FI.

7 PII formats

What forms of PII are covered by the law?

All formats of 'personal data' 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.

8 Extraterritoriality

Is the reach of the law limited to data owners and data processors established or operating in the jurisdiction?

Data protection provisions

No, the data protection provisions under the PDPA generally apply to all organisations that collect, use or disclose personal data in Singapore, whether or not they are formed or recognised under Singapore law, and whether or not they are resident or have an office or place of business in Singapore. As such, organisations which are located overseas are still subject to the data protection provisions so long as they collect, use or disclose personal data in Singapore. In addition, organisations that collect personal data overseas and host and/or process it in Singapore will generally also be subject to the relevant obligations under the PDPA from the point that such data is brought into Singapore.

Do-not-call provisions

Similarly, the DNC provisions under the PDPA apply to all individuals and organisations sending marketing messages to Singapore telephone numbers, as long as either the sender (when the marketing message is sent) or the recipient (when the marketing message is accessed) is present in Singapore. As an example of its application, the requirement to check the DNC registers would not apply to overseas telecoms service operators sending marketing messages to Singapore subscribers roaming on overseas telecoms networks, because these messages would not be sent or accessed in Singapore. However, organisations in Singapore that outsource their telemarketing activities to overseas organisations and authorise the sending of marketing messages should note that they are still responsible for complying with the DNC provisions, as section 36(1) of the PDPA defines a sender to include a person who causes the message or a voice call containing the message to be sent, or authorises the sending of the message or the making of a voice call containing the message.

9 Covered uses of PII

Is all processing or use of PII covered? Is a distinction made between those who control or own PII and those who provide services to owners?

Yes, the PDPA regulates the collection, use and disclosure of personal data by organisations. All organisations which collect, use or disclose personal data are accordingly required to comply with the data protection provisions under the PDPA.

'Data intermediaries', however, are exempt from the majority of the data protection provisions under the PDPA. These refer to organisations which process personal data on behalf of and for the purposes of another organisation (the principal organisation) pursuant to a written contract. Data intermediaries are only required to comply with the rules relating to the protection and retention of personal data (see question 29 for further details), while the principal organisation is subject to the full suite of data protection provisions under the PDPA as if it was processing the personal data itself.

Legitimate processing of PII

10 Legitimate processing – grounds

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

Yes, the processing of personal data is expressed in terms of 'collection, use and disclosure' of the same under the PDPA. 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 given, 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. Fresh consent would need to be obtained where personal data collected is to be used for a different purpose from what the individual originally consented to.

In addition, organisations should note that 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, in order to obtain or attempt to obtain the individual's consent for collecting, using or disclosing personal data.

The PDPA stipulates that consent is deemed to have been given where the following conditions are satisfied:

- 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.

Where an individual has given (or is deemed to have given) consent for the disclosure of his or her personal data by Organisation A to Organisation B for a particular purpose, such individual would also be deemed to have given consent to Organisation B for the collection, use or disclosure of his or her personal data for that particular purpose.

While consent is generally needed, the Second, Third and Fourth Schedule to the PDPA provide for specific situations where personal data can be collected, used or disclosed without the individual's consent.

The Second Schedule to the PDPA allows personal data to be collected without consent, for example, where:

- the collection of personal data is necessary for any purpose that is clearly in the interest of the individual, if consent for its collection cannot be obtained in a timely way or the individual would not reasonably be expected to withhold consent;
- the personal data is publicly available;
- the collection of personal data is necessary for any investigation or proceedings, and if it is reasonable to expect that seeking the consent of the individual would compromise the availability or the accuracy of the personal data;
- the collection of personal data is for the purpose of recovery of a debt owed to the organisation by the individual or for the organisation to pay to the individual a debt owed by the organisation;
- the collection of personal data is necessary for the provision of legal services by the organisation to another person, or for the organisation to obtain legal services;
- the personal data is included in a document produced in the course of, and for the purposes of, the individual's employment, business or profession and collected for the purposes consistent with the purposes for which the document was produced; or
- the personal data is collected by an individual's employer and the collection is reasonable for the purpose of managing or terminating an employment relationship between the organisation and the individual.

The Third Schedule to the PDPA allows personal data to be used without consent, for example, where:

- the use is necessary for any purpose which is clearly in the interests of the individual and:
  - if consent for its use cannot be obtained in a timely way; or
  - the individual would not reasonably be expected to withhold consent;
- the personal data is publicly available;
- the use is necessary for any investigation or proceedings;
- the personal data is used for an organisation to recover a debt owed to the organisation by the individual or for the organisation to pay to the individual a debt owed by the organisation; or
- the use is necessary for the provision of legal services by the organisation to another person, or for the organisation to obtain legal services.

The Fourth Schedule to the PDPA allows personal data to be disclosed without consent, for example, where:

- the disclosure is necessary for any purpose which is clearly in the interests of the individual if consent for its disclosure cannot be obtained in a timely way;
- the personal data is publicly available;
- the disclosure is necessary for any investigation or proceedings;
- the disclosure is necessary for an organisation to recover a debt owed to the organisation by the individual or for the organisation to pay to the individual a debt owed by the organisation;
- the disclosure is necessary for the provision of legal services by the organisation to another person, or for the organisation to obtain legal services; or
- the personal data is disclosed to any officer of a prescribed law enforcement agency, upon production of written authorisation signed by the head or director of that law enforcement agency or a person of a similar rank, certifying that the personal data is necessary for the purposes of the functions or duties of the officer.

11 Legitimate processing – types of data

Does the law impose more stringent rules for specific types of data?

Generally, the PDPA does not distinguish between the types and sensitivities of personal data. However, section 24 of the PDPA requires that an organisation would need to make 'reasonable security arrangements' to protect, and to prevent unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks to personal data in its possession or under its control. 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 (see question 19).

Certain types of personal data are also accorded less stringent rules under the PDPA. For instance, the data protection provisions under the PDPA do not apply to personal data which has been contained in a record that has been in existence for at least 100 years. In addition, personal data pertaining to deceased individuals are also excluded from most of the obligations under the PDPA. In relation to such data, organisations will only be subject to the requirements to make reasonable security arrangements for the protection of such data, and the requirements relating to disclosure of personal data. These reduced obligations will apply for 10 years from the deceased's date of death. In this regard, an individual appointed under the deceased's will to exercise such rights (or, if there is no such person, the deceased's nearest relative) may exercise all or any of the following rights in relation to the protection of the deceased's personal data:

- the right to give or withdraw any consent for the purposes of the PDPA;
- the right to commence a private civil action in respect of any loss or damage suffered from a contravention of any of the provisions under parts IV to VI of the PDPA; and
- the right to bring a complaint under the PDPA.

While the PDPA does not distinguish between the treatment of personal data of minors and that of individuals above 21 years of age, the PDPC has, in its Selected Topics Guidelines, recommended that organisations take appropriate steps to ensure that a minor can effectively give consent on his or her own behalf, in light of the circumstances of the particular case including the impact on the minor in giving consent. In this regard, the PDPC has also indicated that it will adopt the practical rule of thumb that a minor who is at least 13 years of age would typically have sufficient understanding to be able to consent on his or her own behalf. However, where, for example, an organisation has reason to believe or it can be shown that a minor does not have sufficient understanding of the nature and consequences of giving consent, the organisation should obtain consent from an individual who is legally able to provide consent on the minor's behalf (eg, his parent or other legal guardian).

Data handling responsibilities of owners of PII

12 Notification

Does the law require owners of PII to notify individuals whose data they hold? What must the notice contain and when must it be provided?

The obligation to notify stems primarily from the process of seeking valid consent (see question 10). In particular, organisations are obliged to inform individuals of:

(i) the purposes for the collection, use and disclosure of his personal data, on or before collecting the personal data;
(ii) any other purpose for the use or disclosure of personal data which has not been notified to the individual under (i), before such use or disclosure of personal data; and
(iii) on request by the individual, the business contact information of a person who is able to answer the individual's questions about the collection, use and disclosure of the personal data on behalf of the organisation.

Only after the above information has been notified to the individual can he be considered to have validly given his consent to the collection, use and disclosure of his personal data in accordance with the purposes made known to him.

While the 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.

In relation to personal data which was collected by an organisation prior to the data protection provisions under the PDPA coming into effect on 2 July 2014, there is no express requirement under the PDPA that requires the organisation to notify individuals whose personal data they hold. However, fresh consent would need to be obtained from the individual concerned where personal data collected is to be used for a different purpose than what was originally consented to. It follows that notification of the new purposes for which the personal data is to be collected, used or disclosed would also be required.

13 Exemption from notification

When is notice not required?

Generally, the obligation to notify the individual does not apply in situations where the collection, use or disclosure of personal data is authorised under any other written law, or where the individual's consent is deemed to have been given.

In addition, the Second, Third and Fourth Schedules to the PDPA also set out respectively certain circumstances where an individual's consent need not be obtained for the collection, use and disclosure of his personal data (refer to question 10 for more details). Accordingly, the notification obligation would not apply under such circumstances.

However, section 20(4) of the PDPA carves out an exception to this concession. An organisation, on or before collecting, using or disclosing the personal data about an individual for the purpose of managing or terminating an employment relationship has the obligation to inform the individual of that purpose; and, on request by the individual, the business contact information of a person who is able to answer the individual's questions about the collection, use and disclosure on behalf of the organisation. This is despite the fact that the same organisation has no obligation to seek the consent of the individual before collecting, using or disclosing personal data for such purposes.

14 Control of use

Must owners of PII offer individuals any degree of choice or control over the use of their information? In which circumstances?

There is no specific requirement under the PDPA that compels organisations which hold the personal data of individuals to offer such individuals the right to have a degree of choice or control over the use of their personal data.

However, individuals have a right under section 16 of the PDPA to withdraw consent (including deemed consent) given to an organisation in respect of the collection, use or disclosure by that organisation of personal data about the individual for any purpose. The individual would need to give reasonable notice to the organisation as to the withdrawal of his or her consent. Thereafter, upon receipt of such notice, the organisation would need to inform the individual of the likely consequences of the withdrawal of consent, although the organisation should not prohibit the individual from withdrawing consent. Where the individual has withdrawn his or her consent, organisations would be required to inform their data intermediaries and agents to similarly cease collecting, using or disclosing the personal data of an individual who has withdrawn his or her consent to the same.

15 Data accuracy

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

Section 23 of the PDPA generally requires that organisations make a reasonable effort to ensure that personal data that 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 PDPC, in its Key Concepts Guidelines, has stated that an organisation must make a reasonable effort to ensure that:

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

The Key Concepts Guidelines also state that organisations, in deciding what is considered a reasonable effort, should take into account the following factors:

- the nature of the data and its significance to the individual concerned (eg, whether the data relates to an important aspect of the individual such as his or her health);
- the purpose for which the data is collected, used or disclosed;
- the reliability of the data (eg, whether it was obtained from a reliable source or through reliable means);
- the currency of the data (that is, whether the data is recent or was first collected some time ago); and
- the impact on the individual concerned if the personal data is inaccurate or incomplete (eg, based on how the data will be used by the organisation or another organisation to which the first organisation will disclose the data).

16 Amount and duration of data holding

Does the law restrict the amount of PII that may be held or the length of time it may be held?

Yes, section 25 of the PDPA provides that organisations (including data intermediaries) should cease to retain personal data, or remove the means by which 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 in

order 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.

In addition, the PDPC in its Key Concepts Guidelines has clarified that personal data should not be kept by an organisation 'just in case' it may be needed. However, personal data may be retained so long as one or more of the purposes for which it was collected remains valid.

17 Finality principle

Are the purposes for which PII can be used by owners restricted? Has the 'finality principle' been adopted?

Yes, the purposes for which personal data can be used or disclosed by organisations is restricted to the purposes for which the individual concerned had given his or her consent to the organisation in respect of the same.

18 Use for new purposes

If the finality principle has been adopted, how far does the law allow for PII to be used for new purposes? Are there exceptions or exclusions from the finality principle?

Generally, fresh consent would need to be obtained where organisations are seeking to collect, use or disclose personal data for different purposes than those for which the individual concerned had given his or her consent (see question 10).

Security

19 Security obligations

What security obligations are imposed on data owners and entities that process PII on their behalf?

Section 24 of the PDPA requires that organisations make 'reasonable security arrangements' to prevent unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks. Organisations that process personal data on behalf of an organisation (ie, data intermediaries) are also subject to the same requirement. While the PDPC has recognised that there is no one-size-fits-all solution, it has, in its Key Concepts Guidelines, noted that an organisation should:

- design and organise its security arrangements to fit the nature 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.

20 Notification of security breach

Does the law include obligations to notify the regulator or individuals of breaches of security?

There is presently no strict requirement prescribed under the PDPA. However, according to public guidance published on the PDPC's website as of July 2014, one of the mitigating factors which the PDPC may consider when determining a financial penalty to be imposed on an organisation which has breached the PDPA, is whether the organisation voluntarily disclosed the personal data breach to the PDPC as soon as it learned of the breach and co-operated with the PDPC in its investigations.

Internal controls

21 Data protection officer

Is the appointment of a data protection officer mandatory? What are the data protection officer's legal responsibilities?

Yes, section 11 of the PDPA specifically requires that organisations designate one or more individuals to be the organisation's data protection officer. This may be a person whose scope of work solely relates to data protection or a person in the organisation who takes on this role as one of his or her multiple responsibilities. The business contact information of at least one of these data protection officers would need to be made known to the public.

The data protection officer is responsible for ensuring that the organisation complies with the provisions of the PDPA, although the designation of a data protection officer does not relieve an organisation of its obligations and liabilities (in the event of non-compliance of these obligations) under the PDPA.

22 Record keeping

Are owners of PII required to maintain any internal records or establish internal processes or documentation?

Yes, in order to be able to comply with access requests by individuals (see question 34), the Key Concepts Guidelines state that organisations are generally required to implement processes to keep track of the collection, use and disclosure of all personal data under their control, including unstructured data.

Organisations are also required under section 24 of the PDPA to make reasonable security arrangements to prevent unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks to any personal data in their possession or under their control. While the PDPC has recognised that there is no one-size-fits-all solution for organisations, it has, in its Key Concepts Guidelines, noted that an organisation should:

- design and organise its security arrangements to fit the nature 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.

Organisations are also expected to cease retaining documents containing personal data, or remove the means by which personal data is associated with particular individuals, as soon as it is reasonable to assume that the purposes for which the personal data was collected is no longer being served by its retention, or the retention of the same is no longer necessary for legal or business purposes.

Registration and notification

23 Registration

Are owners and processors of PII required to register with the supervisory authority? Are there any exemptions?

No, there is presently no such requirement under the PDPA for organisations that collect, use or disclose personal data to register with the PDPC.

However, individuals may register their Singapore telephone numbers on one of the three DNC registers (for faxes, voice calls, and text messages including SMS/MMS messages and any data applications which use a Singapore telephone number such as 'WhatsApp', 'iMessage' or 'Viber'). From 2 January 2014, individuals and organisations intending to make telemarketing calls or send telemarketing messages (specified messages) are required to check the DNC Registry to ensure that recipient telephone numbers have not been registered before sending such specified messages. In this regard, businesses intending to send specified messages to Singapore telephone numbers are required to check the relevant DNC Registries at least once every 60 days (for messages sent before 1 August 2014), and at least once every 30 days (for messages sent on or after 1 August 2014).

24 Formalities

What are the formalities for registration?

There is presently no requirement under the PDPA for organisations to register with the PDPC.

With regard to the formalities for registration of Singapore telephone numbers on the DNC Registry, individuals may apply to add or remove their Singapore telephone number to or from the registry in any one of three methods:

- by calling a toll-free number to access the automated Interactive Voice Responsive System (IVRS), which will provide step-by-step instructions;

- by sending a text message to a designated number; or
- by registering online through the DNC Registry website.

The registration of a Singapore telephone number on the DNC Registry is free of charge and permanent until withdrawn by the user or subscriber, or until the relevant telecommunications service linked to the number is terminated.

25 Penalties

What are the penalties for a data owner or processor for failure to make or maintain an entry on the register?

There is presently no requirement under the PDPA for organisations to register with the PDPC.

However, organisations which make telemarketing calls or send specified messages are required to check the DNC Registry regularly to ensure that recipient telephone numbers have not been registered on the relevant register, unless they have obtained clear and unambiguous consent in evidential form from the recipients. Failing to do so would be a contravention of the DNC Registry rules under the PDPA, and would amount to an offence for which a fine of up to S$10,000 may be imposed.

26 Refusal of registration

On what grounds may the supervisory authority refuse to allow an entry on the register?

There is presently no requirement under the PDPA for organisations to register with the PDPC.

As for the DNC Registry, only Singapore telephone numbers may be registered. Thus, non-Singapore telephone numbers cannot be registered on any of the DNC registers.

27 Public access

Is the register publicly available? How can it be accessed?

There is presently no requirement under the PDPA for organisations to register with the PDPC.

Organisations which make telemarketing calls or send specified messages are required to check the DNC Registry within 60 days (for messages sent before 1 August 2014) and at least once every 30 days (for messages sent on or after 1 August 2014) before sending any such marketing messages.

To access the DNC Registry to perform a check against the DNC registers, organisations are required to apply for an online account through the DNC Registry website. This is a one-time application which results in the creation of a main account for the organisation. Main account holders can create as many sub accounts as required. Creation of an account is open to organisations registered in Singapore, overseas organisations, and individuals (eg, freelancers and agents who conduct telemarketing activities). Fees are payable for creating main and sub-accounts, as well as for running checks on the DNC Registry.

28 Effect of registration

Does an entry on the register have any specific legal effect?

Organisations collecting, using or disclosing personal data are not presently required to register with the PDPC.

Individuals who register their Singapore telephone numbers on the DNC Registry can expect to stop receiving unsolicited telemarketing messages on their registered telephone numbers 30 days after registration (if they register on or after 2 July 2014) and up to 60 days after registration (if they register before 2 July 2014).

Transfer and disclosure of PII

29 Transfer of PII

How does the law regulate the transfer of PII to entities that provide outsourced processing services?

Organisations that process personal data on behalf of another organisation (the principal organisation) are considered 'data intermediaries' under the PDPA. Such data intermediaries are exempt from most of the main data protection provisions under the PDPA. Data intermediaries are only subject to the data protection provisions relating to the protection and retention of personal data. Specifically, they are required to:

- make reasonable security arrangements to protect personal data in their possession or under their control in order to prevent unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks; and
- anonymise or cease retaining personal data, 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.

The principal organisation is subject to the full suite of data protection obligations under the PDPA as if it were processing the personal data itself.

30 Restrictions on disclosure

Describe any specific restrictions on the disclosure of PII to other recipients.

Disclosure of personal data to other recipients must be in accordance with the applicable requirements under the PDPA (see questions 10 and 12).

Furthermore, in certain circumstances the PDPA restricts an organisation from providing an individual with:

- his or her personal data; or
- information about the ways in which his or her personal data has been or may have been used or disclosed by the organisation within a year before the date of the request, in the situation where such individual has requested access to such personal data or information pursuant to the PDPA. Please refer to question 34 for a list of circumstances under which an individual's right to access his personal data is restricted.

31 Cross-border transfer

Is the transfer of PII outside the jurisdiction restricted?

Yes, section 26 of the PDPA prohibits organisations from transferring personal data out of Singapore except in accordance with requirements prescribed under the PDPA to ensure that organisations provide a standard of protection to the transferred personal data that is comparable to the protection under the PDPA.

Under the PDP Regulations, all organisations transferring personal data from Singapore to countries or territories outside of Singapore are required to ensure that the recipient of such personal data is bound by 'legally enforceable obligations' to provide to the transferred personal data a standard of protection that is at least comparable to the protection accorded under the PDPA. These 'legally binding obligations' include obligations imposed under law, contract, binding corporate rules (for transfers to 'related' organisations), or any other legally binding instrument.

Where the transfer of personal data is pursuant to a contract, contractual clauses are to be contained in a legally binding contract that is enforceable against every receiving organisation under the contract. Such a contract must:

- require the recipient to provide a standard of protection for the personal data transferred to the recipient that is at least comparable to the protection under the PDPA; and
- specify the countries and territories to which the personal data may be transferred under the contract.

Where binding corporate rules are used, these rules must:

- require every related recipient of the transferred personal data to provide a standard of protection for the personal data transferred that is at least comparable to the protection under the PDPA; and
- specify:
  - 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; and
- only be used for recipients that are related to the transferring organisation.

Notwithstanding, a transferring organisation is taken to have satisfied its obligation to ensure that the recipient is bound by legally enforceable

obligations to provide to the transferred personal data a PDPA-comparable standard of protection, where:

- the individual consents to the transfer of the personal data to that recipient in that country or territory, after being provided with a reasonable summary in writing of the extent to which the personal data to be transferred will be protected to a PDPA-comparable standard, provided:
  - such consent was not required by the transferring organisation as a condition of providing a product or service, unless the transfer is reasonably necessary to provide the product or service to the individual; and
  - the transferring organisation did not obtain or attempt to obtain such consent by providing false or misleading information about the transfer, or by using other deceptive or misleading practices;
- the transfer of the personal data to the recipient is necessary for the performance of a contract between the individual and the transferring organisation, or to do anything at the individual's request with a view to the individual entering into a contract with the transferring organisation;
- the transfer of the personal data to the recipient is necessary for the conclusion or performance of a contract between the transferring organisation and a third party which is entered into at the individual's request;
- the transfer of the personal data to the recipient is necessary for the conclusion or performance of a contract between the transferring organisation and a third party if a reasonable person would consider the contract to be in the individual's interest;
- the transfer of the personal data to the recipient is necessary for the personal data to be used:
  - for any purpose which is clearly in the interests of the individual (if consent for its use cannot be obtained in a timely way or the individual would not reasonably be expected to withhold consent);
  - to respond to an emergency which threatens the life, health or safety of the individual or another individual;
  - in the national interest; or
  - disclosed:
    - for any purpose which is clearly in the interests of the individual, if consent for its disclosure cannot be obtained in a timely way;
    - to respond to an emergency that threatens the life, health or safety of the individual or another individual;
    - where there are reasonable grounds to believe that the health or safety of the individual or another individual will be seriously affected and consent for the disclosure of the data cannot be obtained in a timely way (provided that the transferring organisation notifies the individual whose personal data is disclosed of such disclosure and the purposes for such disclosure, as soon as may be reasonably practicable);
    - in the national interest; or
    - for the purpose of contacting the next-of-kin or a friend of any injured, ill or deceased individual;
- the personal data is data in transit (ie, personal data transferred through Singapore in the course of onward transportation to a country or territory outside Singapore, without the personal data being accessed, used by or disclosed to any organisation (other than the transferring organisation or an employee of the transferring organisation) while the personal data is in Singapore, except for the purpose of such transportation); or
- the personal data is publicly available in Singapore.

32 Notification of transfer

Does transfer of PII require notification to or authorisation from a supervisory authority?

No, there is presently no such requirement under the PDPA to notify the PDPC of transfers of personal data.

33 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 PDPA imposes an obligation on organisations transferring personal data out of Singapore to ensure that the recipient of such personal data is bound by 'legally enforceable obligations' to provide to the transferred personal data a standard of protection that is at least comparable to the protection accorded under the PDPA (see question 31). Where organisations use contractual clauses for the purpose of imposing such 'legally enforceable obligations', the PDPC, in its Key Concepts Guidelines, distinguishes between data intermediaries (see questions 9 and 29 for the definition of a 'data intermediary') and all other organisations.

Where the recipient is a data intermediary, the transferring organisation has to set out minimal protections with regard to protection and retention limitation of the personal data.

Where the recipient is an organisation other than a data intermediary, the transferring organisation has to set out protections for the transferred personal data with regard to:

- the purpose of collection, use and disclosure by recipient;
- accuracy;
- protection;
- retention limitation;
- policies on personal data protection;
- access; and
- correction.

The PDPA does not explicitly require transferring organisations to ensure that the 'legally enforceable obligations' imposed on recipients apply to onwards transfers of personal data to third party organisations. However, to the extent that recipients are bound by legally enforceable obligations to provide a PDPA-comparable standard of protection in respect of the transferred personal data, recipients would similarly be obliged to ensure that any onwards transfers of personal data are conducted in accordance with the requirements of the PDPA.

Rights of individuals

34 Access

Do individuals have the right to see a copy of their personal information held by PII owners? Describe any limitations to this right.

Yes, under section 21 of the 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 the ways in which that personal data has been or may have been used or disclosed within a year before the date of request for access.

This individual's right of access is subject to a number of exceptions. 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 identity; or
- be contrary to the national interest.

Further, the Fifth Schedule to the PDPA sets out certain situations where organisations are not required to accede to such requests. For example, organisations need not provide access to personal data or information as to how the personal data has been or may have been used or disclosed, in respect of:

- documents relating to a prosecution if all proceedings related to the prosecution have not been completed;
- personal data which is subject to legal privilege;

- personal data, which if disclosed, would reveal confidential commercial information that could, in the opinion of a reasonable person, harm the competitive position of the 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 information that is trivial; or
  - that is otherwise frivolous or vexatious.

In addition, an organisation must not inform an individual that it has disclosed his or her personal data without his or her consent pursuant to certain exceptions under the Fourth Schedule to the PDPA, namely, where:
- the disclosure is necessary for any investigation or proceedings; or
- the personal data is disclosed to any duly-authorised officer of a prescribed law enforcement agency.

Under the PDP Regulations, organisations are entitled to charge the individual a reasonable fee for access to his personal data. 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. Under the PDPA, organisations are also 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 the 30 days from the request, it is required to inform the individual in writing within that same timeframe of the time by which it will be able to respond to the request (which should be the soonest possible time it can provide access).

35 Other rights

Do individuals have other substantive rights?

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 certain exemptions. For instance, organisations need not correct any error or omission in any personal data about the individual that is in the possession or under the control of the organisation, upon request by the individual concerned if the request relates to:
- opinion data kept solely by the organisation for an evaluative purpose;
- any examination conducted by an education institution, examination scripts and, prior to the release of examination results, examination results;
- personal data of the beneficiaries of a private trust kept solely for the purpose of administering the trust;
- personal data kept by an arbitral institution or a mediation centre solely for the purposes of arbitration or mediation proceedings administered by the arbitral institution or mediation centre; or
- a document related to a prosecution if all proceedings related to the prosecution have not been completed.

Unlike access requests, organisations are not entitled to charge a fee for correction requests. Under the PDPA, 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 timeframe of the time by which it will be able to do so (which should be the soonest practicable time it can make the correction). 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.

The PDPA also provides an individual with the right to commence a private action against an organisation where such an individual has suffered loss or damage directly as a result of non-compliance by the organisation of the data protection provisions under parts IV to VI of the PDPA, subject to certain limitations (see question 36).

36 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, any person who suffers loss or damage directly as a result of non-compliance by an organisation with the data protection provisions under parts IV to VI of the PDPA will have a right of action for relief in civil proceedings in a court. However, where the PDPC has made a decision under the PDPA in respect of such a contravention, this right is only exercisable after such a decision issued by the PDPC has become final after all avenues of appeal have been exhausted. The court may grant relief as it thinks fit, including an award of an injunction or declaration, or damages.

37 Enforcement

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

The right to commence a private action for loss or damage suffered as a result of an organisation's non-compliance with the PDPA would be an action for relief in civil proceedings. As mentioned, however, such right is only exercisable provided that any relevant infringement decision issued by the PDPC has become final after all avenues of appeal have been exhausted.

Therefore, if an individual becomes aware that an organisation has failed to comply with the PDPA, such individual may lodge a complaint to the organisation directly, or bring a complaint to the PDPC. Upon receipt of a complaint, the PDPC may then investigate or review the matter, or direct the parties as to the appropriate mode of dispute resolution.

Where the PDPC is satisfied that an organisation has breached the data protection provisions under the PDPA, the PDPC is empowered with a 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 or correct personal data; or
- pay a financial penalty of up to S$1 million.

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 where such decision relates to the amount of a financial penalty. Reconsideration applications and appeal requests must be made within 28 days of 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.

Exemptions, derogations and restrictions

38 Further exemptions and restrictions

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

The application of the data protection provisions does not extend to 'business contact information', 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 personal purposes'.

Update and trends

PDPA comes into full effect

On 2 July 2014, the PDPA took full effect, with the coming into effect of the data protection provisions establishing Singapore's first general data protection law. The PDPA imposes a number of obligations on organisations that collect, use and disclose personal data. With the coming into effect of the data protection provisions, organisations that collect, use or disclose the personal data of individuals for any particular purpose(s) must ensure that they notify individuals and obtain their consent for such purpose(s), unless a relevant exception applies. Organisations must also comply with other obligations under the PDPA.

To provide clarity on specific obligations and issues under the PDPA, the PDPC has issued a number of advisory guidelines. On 16 May 2014, the PDPC revised its Key Concepts Guidelines to include new chapters dealing with cross-border transfers of personal data, and individuals' access and correction rights. The PDPC also revised its Selected Topics Guidelines to include a new chapter dealing with data activities relating to minors. At the same time, the PDPC also issued sector-specific advisory guidelines relating to the telecommunication sector and the real estate sector, to address unique issues encountered concerning the respective sectors.

At the time of writing, the PDPC has released a number of proposed advisory guidelines under the PDPA for public consultation, which are yet to be finalised. These are sector-specific advisory guidelines for the education, healthcare and social service sectors, as well as advisory guidelines dealing with the topic of photography. When finalised, the guidelines can be expected to provide further clarity on organisations' obligations under the PDPA.

PDPC enforcement of DNC provisions

Following the coming into effect of the DNC provisions in the PDPA on 2 January 2014, the PDPC has commenced enforcement action against a number of organisations for breaching the DNC provisions. According to a media statement issued by the PDPC on 23 May 2014, it has undertaken investigations in response to 3,700 valid complaints from members of the public against 630 organisations since the DNC provisions took effect.

The PDPC has also commenced its first prosecution for offences under the DNC provisions, against tuition agency Star Zest Home Tuition Pte Ltd and its director. The PDPC announced in its media statement that it had received and investigated many complaints relating to unsolicited telemarketing messages allegedly sent by the tuition agency to Singapore telephone numbers which had been registered with the DNC Registry. Under the DNC provisions, a person or organisation found guilty of the offence of sending telemarketing calls or messages to Singapore telephone numbers without checking the DNC Registry is liable to a fine of up to S$10,000 per message sent.

In addition, the PDPC announced that two organisations have accepted offers to compound their offences relating to the sending of telemarketing messages to Singapore telephone numbers, in lieu of prosecution. The composition amounts ranged from S$500 to S$1,000. The PDPC has also issued warning notices to 380 other organisations facing isolated complaints for sending unsolicited telemarketing messages.

In a statement, the PDPC said that it is serious about ensuring compliance with the DNC provisions in the PDPA, and that it will continue to monitor compliance with the requirements in the PDPA, including those relating to data protection.

In addition, organisations are allowed to continue using (which could include disclosure that is necessarily part of such use) personal data collected before the data protection provisions take effect on 2 July 2014, for the purposes for which the personal data was collected, unless consent for such use is withdrawn or the individual indicates or has indicated to the organisation that he does not consent to the use or disclosure of the personal data.

In relation to the DNC provisions, the following messages are excluded from the meaning of a specified message under the Eighth Schedule to the PDPA and therefore not subject to the application of the DNC provisions:

- any message sent by a public agency under, or to promote, any programme carried out by any public agency which is not for a commercial purpose;
- any message sent by an individual acting in a personal or domestic capacity;
- any message which 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 with respect to 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 in relation to a subscription, membership, account, loan or comparable ongoing commercial relationship involving the ongoing purchase or use by the recipient of goods or services offered by the sender, the sole purpose of which is to provide:
  - notification concerning a change in the terms or features;
  - notification of a change in the standing or status of the recipient; or
  - at regular periodic intervals, account balance information or other type of account statement;
- 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.

In addition, the Personal Data Protection (Exemption from section 43) Order 2013 exempts individuals and organisations sending specified messages to Singapore telephone numbers from the requirement to check the DNC Registry, where they have an ongoing business relationship with the subscribers or users of those Singapore telephone numbers. However, the application of the exemption is subject to a number of conditions:

- at the time of the transmission of the specified message, the sender has to be in an ongoing relationship with the recipient;
- the purpose of the specified message has to be related to the subject of the ongoing relationship;
- only specified text and fax messages may be sent to the recipient. Specified messages sent by way of voice calls are not covered by the exemption; and
- the specified message has to contain an opt-out facility for recipients to give an opt-out notice to opt out of any exempt message from the sender.

Supervision

39 Judicial review

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

Yes. However, organisations aggrieved by the PDPC's decision or direction must first:

- request the PDPC to reconsider its decision or direction and thereafter appeal to the Data Protection Appeal Panel; or
- appeal directly to the Data Protection Appeal Panel without submitting a reconsideration request.

Only if such organisation is still aggrieved by the decision of the Data Protection Appeal Panel may it appeal against the Data Protection Appeal Panel's decision to the High Court. An appeal to the High Court can only be made on limited grounds, namely on a point of law or where such decision relates to the amount of a financial penalty.

40 Criminal sanctions

In what circumstances can owners of PII be subject to criminal sanctions?

The following circumstances can trigger criminal sanctions under the PDPA:

- a person who makes a request to obtain access to or to change the personal data of another individual without the authority of that individual commits an offence for which he would be liable on conviction to a fine not exceeding S$5,000 and/or to imprisonment for a term not exceeding 12 months;
- an organisation or person who disposes of, alters, falsifies, conceals or destroys personal data, or information about the collection, use or

disclosure of personal data, with an intent to evade an access request or a correction request commits an offence for which it would be liable upon conviction to a fine of up to S$5,000 (in the case of individuals) or up to S$50,000 (in any other case). For more details on access and correction requests, please see questions 34 and 35 respectively; and
- an organisation or person who obstructs or impedes the PDPC or an authorised officer, or knowingly or recklessly makes a false statement to the PDPC, or knowingly misleads or attempts to mislead the PDPC in the exercise of their powers or performance of their duties under the PDPA, commits an offence that is liable upon conviction to a fine of up to S$10,000 and/or to imprisonment for a term of up to 12 months (in the case of an individual) or a fine of up to S$100,000 (in any other case).

In addition, the PDPA provides that officers/partners of bodies corporate/partnerships will be guilty of the same offence committed by such bodies corporate/partnerships, and liable to be proceeded against and punished accordingly, where the offence is proven to:
- have been committed with the consent or connivance of such officer/partner; or
- be attributable to any neglect on the part of such officer/partner.

Further, the following circumstances may attract criminal sanctions under the DNC provisions of the PDPA:
- a telecommunications service provider which fails to report all Singapore telephone numbers that have been terminated from the relevant DNC registers, in the manner and form prescribed by the PDPC, would be guilty of an offence for which it would be liable to a fine of up to S$10,000 upon conviction;
- any person who fails to check the DNC Registry before sending marketing messages, and who has not obtained the clear and unambiguous consent of the recipient in evidential form, commits an offence and would be liable to a fine of up to S$10,000 upon conviction;
- the failure to include clear and accurate information identifying the sender of the marketing message and on how the recipient may contact the sender is an offence for which the sender would be liable to a fine of up to S$10,000 upon conviction. Additionally, the information included in the message has to be reasonably valid for at least 30 days after the message is sent; and
- the act of concealing or withholding the calling identity of the sender from the recipient of a marketing message is also an offence for which the sender would be liable to a fine of up to S$10,000 upon conviction.

41 Internet use

Describe any rules on the use of 'cookies' or equivalent technology.

The 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. However, the Selected Topics Guidelines clarify that there may not be a need to seek consent for the use of cookies to collect, use and disclose personal data 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 (but are not limited to) 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 if the individual voluntarily provides the personal data for that purpose of the activity, and it is reasonable that he 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 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.

In addition, the Selected Topics Guidelines makes clear that where organisations use cookies for behavioural targeting that involves the collection and use of an individual's personal data, the individual's consent is required.

42 Electronic communications marketing

Describe any rules on marketing by e-mail, fax or telephone.

Organisations which make telemarketing calls or send messages of a commercial nature are required to check the DNC Registry within 60 days (for messages sent before 1 August 2014) and at least once every 30 days (for messages sent on or after 1 August 2014) before sending any such marketing messages, unless they have obtained clear and unambiguous consent from the recipients in evidential form. Please see question 27 for details on how checks on the DNC Registry can be conducted.

Regarding the rules on marketing by e-mail, the Spam Control Act governs the sending of unsolicited e-mails or spam in Singapore. For more details on the specifics of contravening these rules, please see question 5.

DREW & NAPIER

Lim Chong Kin **chongkin.lim@drewnapier.com**
Charmian Aw **charmian.aw@drewnapier.com**

10 Collyer Quay #10-01
Ocean Financial Centre
Singapore 049315

Tel: +65 6531 4110
Fax: +65 6535 4864
www.drewnapier.com

Getting the Deal Through

Acquisition Finance
Advertising & Marketing
Air Transport
Anti-Corruption Regulation
Anti-Money Laundering
Arbitration
Asset Recovery
Aviation Finance & Leasing
Banking Regulation
Cartel Regulation
Climate Regulation
Construction
Copyright
Corporate Governance
Corporate Immigration
Data Protection & Privacy
Debt Capital Markets
Dispute Resolution
Domains and Domain Names
Dominance
e-Commerce
Electricity Regulation
Enforcement of Foreign Judgments
Environment
Foreign Investment Review
Franchise
Gas Regulation
Government Investigations
Insurance & Reinsurance
Insurance Litigation
Intellectual Property & Antitrust
Investment Treaty Arbitration
Islamic Finance & Markets
Labour & Employment
Licensing
Life Sciences
Mediation
Merger Control
Mergers & Acquisitions
Mining
Oil Regulation
Outsourcing
Patents
Pensions & Retirement Plans
Pharmaceutical Antitrust
Private Antitrust Litigation
Private Client
Private Equity
Product Liability
Product Recall
Project Finance
Public-Private Partnerships
Public Procurement
Real Estate
Restructuring & Insolvency
Right of Publicity
Securities Finance
Ship Finance
Shipbuilding
Shipping
State Aid
Tax Controversy
Tax on Inbound Investment
Telecoms and Media
Trade & Customs
Trademarks
Transfer Pricing
Vertical Agreements

Also available digitally

Online

www.gettingthedealthrough.com

iPad app

Available on iTunes

Law Business Research

Data Protection & Privacy
ISSN 2051-1280

THE QUEEN'S AWARDS FOR ENTERPRISE: 2012

LACCA
LATIN AMERICAN CORPORATE COUNSEL ASSOCIATION

Official Partner of the Latin American Corporate Counsel Association

ABA Section of International Law
Your Gateway to International Practice

Strategic Research Partner of the ABA Section of International Law