A GLOBAL ROADMAP TO PERSONAL DATA PROTECTION

Asia Pacific, Europe & USA

First Edition

MERITAS®
LAW FIRMS WORLDWIDE

A GLOBAL ROADMAP TO PERSONAL DATA PROTECTION

Asia Pacific, Europe & USA

Dennis Unkovic, Editor

du@muslaw.com
Tel: +1-412-456-2833

Meyer, Unkovic & Scott LLP
www.muslaw.com

Not so long ago, "data protection" meant a locked filing cabinet and a good shredder. No longer. In a single generation, protecting data went from safeguarding documents to securing information of almost every kind, both tangible and in electronic form. Although everyone understands what it means to protect a hard copy document, it is much harder to conceptualize protecting intangible information. To make matters worse, a data breach today can cause far more serious consequences than in years past. To cite just one example, the improper disclosure of one's personal data can easily result in identity theft, with the victim often left unaware of the crime until it is far too late to stop it.

With the endless march of technology and an increasingly connected world, protecting personal data is clearly more important than ever. In response, governments around the world have focused on enacting legislation to keep up with the fast pace of change. The EU's recent implementation of the General Data Protection Regulation (GDPR) is just the latest development in this crucial area of law. Outside the EU, however, there is little uniformity in how different regions and countries protect personal data. To help make sense of this, Meritas® has produced this guide by leveraging its top quality member firms from around the world, specifically our firms in Asia Pacific, Europe and the USA. The guide employs a straightforward question-and-answer format to be as simple and as easy to use as possible. The authors hope that this guide will provide readers with a convenient and practical starting point to understand a complicated yet vitally important subject to businesses everywhere.

Special thanks go out to Meritas® Board Member Yao Rao (China), who was the inspiration behind this publication, as well as to Meritas® Board Member Darcy Kishida (Japan) and Eliza Tan (Meritas® Asia Regional Representative), who provided crucial support. Without their hard work and dedication, this global look at the critical issue of Data Privacy would not have been published.

ABOUT MERITAS®

Founded in 1990, Meritas® is the premier global alliance of independent law firms working collaboratively to provide businesses with qualified legal expertise. Our market-leading member firms offer a full range of high-quality, specialized legal services, allowing you to confidently conduct business anywhere in the world.

As an invitation-only alliance, Meritas® firms must adhere to our uncompromising service standards to retain membership status. Unlike any other network or law firm, Meritas® collects peer-driven reviews for each referral, and has for more than 25 years.

7,500+ EXPERIENCED LAWYERS

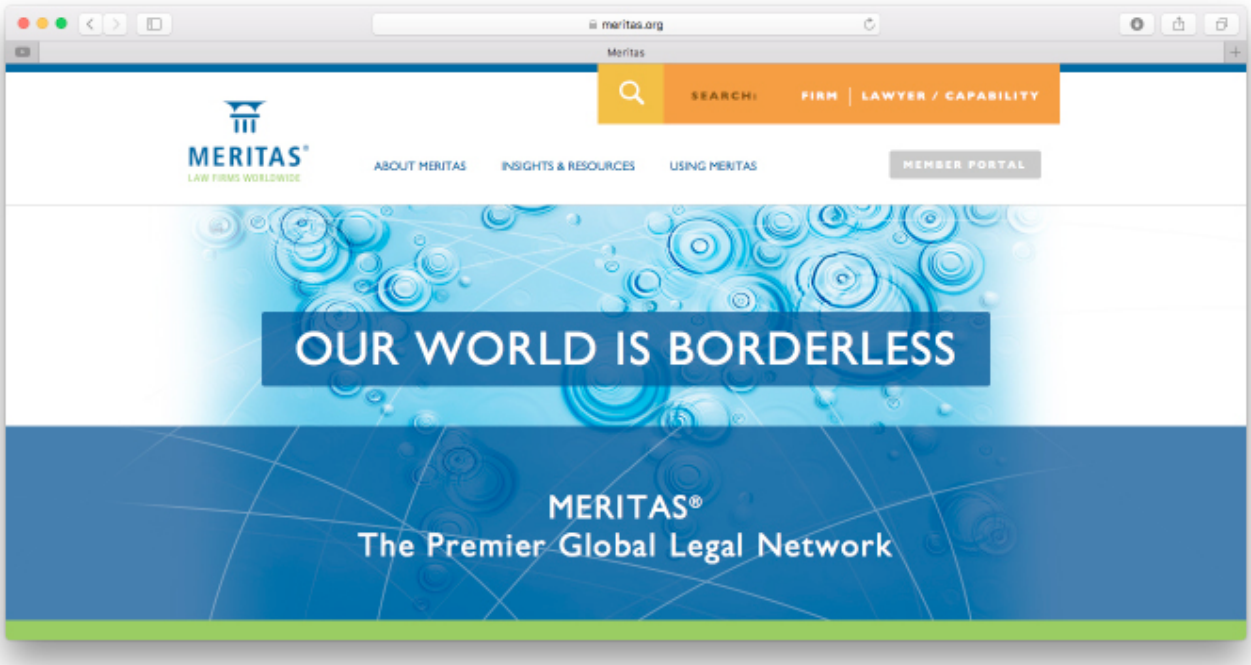
90+ COUNTRIES

180+ LAW FIRMS

240+ GLOBAL MARKETS

Using this exclusive ongoing review process, Meritas® ensures quality, consistency and client satisfaction.

With 180+ top-ranking law firms spanning more than 90 countries, Meritas® delivers exceptional legal knowledge, personal attention and proven value to clients worldwide.



For more information visit:

MERITAS®
LAW FIRMS WORLDWIDE

www.meritas.org

MERITAS®
LAW FIRMS WORLDWIDE

SINGAPORE

FIRM PROFILE:

JOYCE A TAN & PARTNERS

The firm provides the full range of corporate and commercial legal services with particular strengths in intellectual property, information technology, telecommunications, media and entertainment.

The firm's service philosophy is aimed at bringing clarity to a situation and making the client experience a seamless, fuss-free encounter across multiple requirements that may arise. The firm does this by the pre-emptive, integrated and commercially realistic approach to the work and strategies it undertakes and ensuring alignment with its clients. The key areas of the firm's practice comprises work in:

- Corporate and Commercial Transactions
- Private Equity and Investment
- Business Financing
- Company Regulatory Compliance
- Employment and Immigration
- Intellectual Property
- Information Technology
- Telecommunications and Broadcasting
- Media and Publishing
- Entertainment
- Dispute Management and Litigation
- Arbitration, Mediation and Other Alternative Dispute Resolution
- Family and Personal Law

The firm routinely operates in a cross-border setting, managing local and foreign elements and dimensions as second nature, with its strong and keen multi-jurisdictional awareness and approach to the matters it handles.

CONTACT:

JOYCE A.TAN
joyce@joylaw.com

DANIEL LIM
daniel@joylaw.com

+65 6333 6383
www.joylaw.com

Introduction

In Singapore, the mandatory protection of "personal data" (as is the term used, rather than "personal information") under specific legislation only came into force in 2014, with the promulgation of the Personal Data Protection Act 2012 ("**PDPA**"). This protection regime seeks to address growing concerns from individuals about how their personal data is being used, maintain the trust of individuals in organisations that manage data, and strengthen Singapore's position as a trusted business hub.

1. What are the major personal information protection laws or regulations in your jurisdiction?

Putting aside common law remedies (e.g. breach of confidence, etc.), sector-specific legislation (e.g. Official Secrets Act, Banking Act, etc.) and industry-specific self-regulatory codes (e.g. Singapore Code of Advertising Practice), personal data is primarily protected by the PDPA, which:

(1) Governs the collection, use, disclosure and care of personal data by an "organisation" (which includes any individual or legal entity) in a manner which recognises both –

- The needs of organisations to collect, use or disclose personal data for legitimate and reasonable purposes; and
- The rights of individuals to protect their personal data;

(2) Includes a national Do Not Call Registry, which allows individuals to opt out of receiving marketing phone calls, mobile text messages, and faxes from organisations; and

(3) Is supplemented by various –

- subsidiary legislation comprising the
  - Personal Data Protection (Do Not Call Registry) Regulations 2013;
  - Personal Data Protection (Composition of Offences) Regulations 2013;
  - Personal Data Protection Regulations 2014;
  - Personal Data Protection (Enforcement) Regulations 2014;
  - Personal Data Protection (Appeal) Regulations 2015;
- Practical tools issued by the Personal Data Protection Commission ("**PDPC**") comprising
  - Advisory Guidelines on PDPC's interpretation of PDPA provisions and handling of general and sector-specific issues; and
  - General Guides to assist organisations in complying with the PDPA.

2. How is "personal information" defined?

Under the PDPA, "personal data":

(1) Is defined 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";

(2) May include different types of data about an individual and from which an individual can be identified, such as the individual's passport number, facial image, voice, fingerprint, or DNA profile, regardless of such data being true or false or whether the data exists in electronic or other form; and

(3) Excludes –

- Business contact information e.g. position name or title, business telephone number, address, email and other similar information not provided by the individual solely for personal purposes; and
- Personal data contained in a record in existence for at least 100 years, or about an individual who has been dead for more than 10 years.

3. What are the key principles relating to personal information protection?

The PDPA is based on the following principles:

(1) ***Accountability***: An organisation is responsible for personal data in its possession or under its control. Where personal data is under the control of the organisation, the organisation shall designate one or more individuals to be responsible for compliance under the PDPA.

(2) ***Specified purpose/s***: The purpose/s for which personal data is collected by an organisation shall be specified by the organisation.

(3) ***Consent***: An individual's consent is required for the collection, use, or disclosure of his personal data, save in exceptional cases where the individual may be deemed to consent or where no consent is required.

(4) ***Reasonable* collection**: The collection of personal data shall be limited to that which is necessary for the specified purpose/s that a reasonable person would consider appropriate in the circumstances.

(5) ***Authorised use, disclosure, and retention***: Personal data shall not be used or disclosed to a third party for purposes other than the specified purpose/s for which it was collected, unless the individual consents to such use or disclosure, or unless exceptions allow for use or disclosure without consent. Personal data shall be retained only as long as necessary for the fulfillment of the specified purpose/s.

(6) ***Accuracy***: An organisation shall make a reasonable effort to ensure that personal data collected is accurate and complete if the personal data is likely to be used to make a decision affecting the individual to whom the data relates or is likely to be disclosed by the organisation to another organisation.

(7) ***Safeguards***: An organisation shall protect personal data in its possession or under its control by making reasonable security arrangements to prevent unauthorised access, collection, use, disclosure, copying, modification, disposal, or similar risks.

(8) ***Openness***: An organisation shall make available information about (a) policies and practices necessary for the organisation to meet its obligations under the PDPA; and (b) information about the complaint process to receive and respond to complaints that may arise.

(9) ***Individual access and correction***: An organisation shall, on the request of an individual, provide that individual with personal data about the individual in its possession or control and ways in which that personal data may have been used or disclosed within a year before the date of the request. There are exceptions where an organisation is not required to or shall not provide an individual with the requested personal data. An individual may request an organisation to correct an error or omission in personal data about him and which is in the possession or under the control of the organisation.

(10) ***Manageable compliance costs***: The PDPA aims to keep compliance costs manageable for businesses, especially Small and Medium Enterprises (SMEs). In line with this, a complaints-based approach rather than a more stringent audit-based regime will be adopted. There is no mandatory breach notification requirement under the law, but notification is recommended, as discussed below.

(11) ***Consistency with international standards***: The data protection regime is designed to be in line with international standards for data protection, such as the OECD Guidelines and the data protection frameworks in key jurisdictions, including Canada, New Zealand, Hong Kong, and the European Union.

(12) ***Facilitate cross-sector data flows***: The PDPA aims to be a general baseline law that applies across all sectors. It coexists with sector-specific regulations, which may impose more stringent data protection requirements. A baseline law engenders greater consumer trust in the private sector while at the same time facilitating data flows to achieve positive economic outcomes.

4. What are the compliance requirements for the collection of personal information?

Unless the collection is required or authorised by law or under

certain prescribed exceptional circumstances e.g. an emergency that threatens the life, health or safety of the individual to whom the personal data relates or any other individual, an organisation which collects personal data about an individual is obliged to ensure that:

(1) The organisation shall have notified the individual of the purpose/s for which his personal data will be collected – the form and manner of such notification is to be determined by the organization as the best way of doing so, generally regarded as being in written form (whether electronic or other documented form) so that the individual is clear about the purpose/s and the parties have clear documentation on the matter to refer to in the event of any dispute;

(2) The individual's consent to the collection for such purpose/s has been given, which would be –

- Deemed to have been given if he voluntarily provides the personal data to the organisation, and it is reasonable that the individual would voluntarily provide the personal data;
- Invalid if the organisation –
  - As a condition of providing a product or service, had required the individual to consent to the collection of personal data beyond what is reasonable to provide the product or service to the individual; or
  - Had obtained or attempted to obtain the said consent by providing false or misleading information, or using deceptive or misleading practices.

5. What are the compliance requirements for the processing, use and disclosure of personal information?

(1) The requirements for the use and disclosure of personal data are identical to those set out at in the response to Question 4 above, in relation to the collection of personal data.

(2) In addition, an organisation in possession of personal data is obliged to:

- Make a reasonable effort to ensure that the personal data collected is accurate and complete, if the personal data is likely to be used by the organisation in making a decision that would affect the individual or to be disclosed by the organisation to another organisation;
- Make reasonable security arrangements to protect the personal data, such as preventing unauthorised access, use or disclosure; and
- Cease to retain documents containing personal data, or remove the means by which the personal data can be associated with the particular individual, as soon as it is reasonable to assume that –
  - The purpose for which the personal data was collected is no longer being served by retention of the personal data; and
  - Such retention is no longer necessary for legal or business purposes (there is no specified duration for this, which is assessed on a standard of reasonableness, having regard to the purposes for which the personal data was collected and other legal or business purposes for which its retention may be necessary).

(3) A data intermediary, i.e. an organisation which processes personal data on behalf of another organisation is also obliged to comply with the above security and removal obligations.

6. Are there any restrictions on personal information being transferred to other jurisdictions?

An organisation is not permitted to transfer an individual's personal data to another country or territory outside of Singapore unless it has taken appropriate steps to:

(1) Ensure that it will comply with its obligations on the collection, use and disclosure of the personal data (as set out in the responses to Questions 4 and 5 above), while the transferred personal data remains in its possession or under its control; and

(2) Ascertain whether, and ensure

that, the recipient in that country or territory outside Singapore is bound by legally enforceable obligations (e.g. by any law, contract or binding corporate rules) to protect that personal data at a standard that is at least comparable to that under the PDPA, an obligation which would be considered satisfied if –

- The transferring organisation
  - Duly obtained the individual's consent to the transfer after having provided the individual with a reasonable written summary of the extent to which the personal data transferred will be protected to a standard comparable to that under the PDPA; and
  - Had not required the individual's consent to the transfer as a condition of providing any product or services to the individual (unless the transfer is reasonably necessary to provide such product or service to the individual); and
  - Had not obtained nor attempted to obtain the individual's consent by providing false or misleading information about the transfer, or by using other deceptive or misleading practices; or
- The transfer 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; or
  - The conclusion or performance of a contract between the transferring organisation and a third party which is entered into at the individual's request or if a reasonable person would consider the contract to be in the individual's interest; or
  - The personal data transferred to be used or disclosed in certain prescribed exceptional circumstances where the consent of the individual is not required e.g. an emergency that threatens the life, health or safety of the individual to whom the personal data relates or any other individual, and the organisation has taken reasonable steps to ensure that the personal data will not be used or disclosed by the recipient for any other purpose.

7. What are the rights of an individual whose personal information is collected? Can he/she withdraw the consent to the retention of his/her personal information by a third party, and if so, how?

An individual is entitled to:

(1) Request (other than in exceptional circumstances, such as where the provision would threaten the safety of, or cause immediate harm to, another individual) an organisation, which would be obliged on such request (for which a reasonable fee may be charged), to ***provide the individual*** with –

- Personal data about the individual 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 by the organisation within a year before the date of the individual's request;

(2) Request an organisation in possession or control of his personal data, to ***correct an error or omission*** in such personal data, in which case, unless the organisation is satisfied on reasonable grounds that the correction should not be made, it must (without imposing any charge) –

- Correct the personal data as soon as practicable;
- Send the corrected personal data to every other organisation to which the personal data was disclosed by the organisation within a year before the date of the individual's request, unless that other organisation does not need the corrected personal data for any legal or business purpose; and

- Inform the individual in writing, within 30 days of receiving his request, of the time by which it will be able to correct the personal data, if it is unable to do so within such period of 30 days.

(3) ***Withdraw his consent*** given or deemed to have been given for an organisation's collection, use or disclosure of his personal data for any purpose, by giving reasonable notice of such withdrawal to the organisation, which –

- Must on receipt of the notice
  - Inform the individual of the likely consequences of withdrawing consent; and
  - Cease (and cause its data intermediaries and agents to cease) collecting, using or disclosing the personal data;
- Is, however, not required to delete or destroy the personal data upon request of the individual, but remains obliged to cease retention of, or to remove any means of associating the individual with, the personal data in the circumstances stated at point (2) under Question 5 above; and

(4) A right of action in civil proceedings in a court on account of any loss or damage suffered by the individual directly as a result of an organisation's contravention of its obligations in relation to the collection, use, disclosure, grant of access, correction and care of the individual's personal data –

- For relief, including
  - By way of injunction or declaration;
  - In the form of damages; and/or
  - Such other relief as the court thinks fit.
- Provided that if the PDPC has made a decision on the same contravention, such decision has become final after the right of appeal against that decision has been exhausted.

8. Is an employee's personal information protected differently? If so, what's the difference? Apart from the personal information of employees, are there any other types of personal information that receive special protection?

(1) Subject to any applicable legal obligations, including confidentiality obligations and those under the employment contract:

- The PDPA allows an organisation to collect, use and/or disclose the personal data of an employee or prospective employee, as the case may be, without his consent where –
  - Such collection, use and/or disclosure is necessary for evaluative purposes, which includes determining the suitability, eligibility or qualifications of the employee for promotion or continuance in employment; or
  - Such collection, and subsequent use and/or disclosure, is reasonable for the purpose of managing or terminating the employment relationship with the employee.
- The Employment Act obliges an employer to –
  - Keep a record of complete and accurate information about its employment of every employee and former employee containing various prescribed particulars, including certain personal data ("**employee record**");
  - Retain such employee record relating to the personal data for the duration of employment, and if applicable, one year after the employment ends ("**retention period**"); and
  - Ensure that during such retention period, the employee record is readily accessible to the employee or former employee, as the case may be.

(2) Other than the above, the PDPA does not make any other differentiation of the types of personal data, although in its Advisory Guidelines and decisions, the PDPC has:

- Recognised that certain types of personal data, e.g. bank account details, would typically be more sensitive in

nature; and

- Recommended that organisations –
  - Accord a higher standard of protection to and take relevant precautions in the collection, use and/or disclosure of more sensitive personal data, when making security arrangements to protect personal data under its possession or control; and
  - Take extra steps to verify the accuracy of personal data where inaccuracy of the personal data would have severe consequences on the relevant individual e.g. a minor.

9. Which regulatory authorities are responsible for implementation and enforcement of personal information protection laws in your jurisdiction?

The PDPC is the authority responsible for the administration and enforcement of the PDPA, which may for such purpose, appoint the following:

(1) The Commissioner for Personal Data Protection; and

(2) Such number of Deputy Commissioners for Personal Data Protection, Assistant Commissioners for Personal Data Protection and inspectors, as the PDPC considers necessary.

More information about the PDPC, including its contact details, enforcement actions, etc. may be found at its website at https://www.pdpc.gov.sg.

10. Are there any penalties, liabilities or remedies if any of the personal information protection laws is violated?

Contravention of any personal data protection provisions in the PDPA may:

(1) Incur the PDPC's ***enforcement action*** in the form of such directions as the PDPC thinks fit to ensure compliance with the PDPA (which are subject to an appeal process) including requiring the non-compliant organisation to –
- Stop collecting, using or disclosing personal data in contravention of the PDPA;
- Destroy personal data collected in contravention of the PDPA;
- Comply with the PDPC's finding on the matter of a disputed request by an individual for access to or correction of his personal data as discussed at points (1) and (2) under Question 7 above; and/or
- Pay a financial penalty of an amount not exceeding SGD1 million.

(2) Open the non-compliant organisation to a ***civil suit*** in the court by an individual who suffers loss or damage directly as a result of the contravention, as discussed at point (4) under Question 7 above; and/or

(3) In specific instances, constitute an offence under the PDPA, such as where a person –
- Makes a request to an organisation in order to obtain access to or change the personal data of an individual without the authority of that individual, for which the guilty person would be liable on conviction to –
  - A fine not exceeding SGD5,000; and/or
  - Imprisonment for a term not exceeding 12 months; or
- Disposes of, alters, falsifies, conceals or destroys a record containing personal data or information about the collection, use or disclosure of personal data (or directs another person to do so), for which the guilty person would be liable on conviction to a fine not exceeding –
  - SGD5,000 in the case of an individual; or
  - SGD50,000 in the case of a non-individual.

11. Is your jurisdiction planning to pass any new legislation to protect personal information? How is the area of personal information protection expected to develop in your jurisdiction?

(1) The PDPC recently concluded, in June 2018, its conduct of a public consultation exercise on:
- A review of the Do Not Call provisions of the PDPA to ensure that these provisions

remain relevant in light of the increasing adoption of digital marketing tools such as social media and instant messaging platforms; and

- The introduction of an Enhanced Practical Guidance framework –
  - For the PDPC to provide guidance with regulatory certainty, which the current guidelines do not provide; and
  - Which is intended to facilitate the development of new and innovative data services, recognising the opportunities for innovations around the use of data as Singapore gears up to be a Digital Economy.

(2) Based on public feedback on the above issues, the PDPC might propose amendments to the PDPA, and/or the introduction of new regulations to put in place the Enhanced Practical Guidance framework.

Prepared by Meritas Law Firms

Meritas is an established alliance of 180+ full-service law firms serving over 240 markets – all rigorously qualified, independent and collaborative. Connect with a Meritas law firm and benefit from local insight, local rates and world-class service.

www.meritas.org enables direct access to Meritas law firms through a searchable database of lawyer skills and experience.

MERITAS®
LAW FIRMS WORLDWIDE

www.meritas.org

800 Hennepin Avenue, Suite 600
Minneapolis, Minnesota 55403 USA
+1.612.339.8680