SME guide to the personal data protection act 2012
introduction
to the Personal Data Protection Act 2012

The Personal Data Protection Act 2012 (PDPA) lays out a framework regarding personal data protection for private organisations. With the vast amount of personal data that organisations collect daily, it is important that organisations comply with the PDPA. Organisations may choose to engage external legal advice to ensure compliance with PDPA obligations.¹

There are nine obligations imposed by the Personal Data Protection Act 2012 (PDPA) that has to be adhered to by organisations. They do not, however, apply to the following:

- An individual acting in a personal or domestic capacity;
- An employee acting in the course of his or her employment with an organisation; and
- A public agency or an organisation in the course of acting on behalf of a public agency in relation to the collection, use or disclosure of the personal data.

The DNC Provisions apply both to individuals and organisations, containing obligations pertaining to the sending of specific messages to Singapore telephone numbers. To manage unsolicited telemarketing phone calls, the DNC Registry was established.

The PDPA is administered and enforced by the Personal Data Protection Commission (PDPC), which provides training materials and further guidelines on the PDPA.²

---

¹ Refer to list of resources below for the link to the Legal Advice Scheme by the Law Society of Singapore
² Further materials can be found in the list of resources below
## Personal Data Protection Obligations

1. **Consent Obligation**
   - Prior consent must be obtained from the individual and allowed to withdraw such consent

2. **Purpose Limitation Obligation**
   - Personal data can only be used for the purpose which was consented to by the individual

3. **Notification Obligation**
   - Notify individuals of purpose for collecting personal data on or before collection

4. **Access and Correction Obligation**
   - Provisions should be made to access and correct personal data

5. **Accuracy Obligation**
   - Ensure that personal data is accurate and complete

6. **Protection Obligation**
   - Make reasonable security arrangements to protect personal data

7. **Retention Obligation**
   - Cease retention of personal data when there is no legal or business purpose

8. **Transfer Limitation Obligation**
   - Personal data should only be transferred in accordance with the requirements of the PDPA

9. **Openness Obligation**
   - Make personal data protection policies and complaint process publicly available
1, 2, & 3. consent, purpose limitation and notification obligations

Illustration of personal data

- Personal data is any data, regardless of its accuracy, about an individual who can be identified from that data alone or with other information that an organisation has or is likely to have.

These include:
- NRIC or FIN number
- Passport number
- Photograph or video image of an individual
- Mobile telephone number
- Personal email address
- Thumbprint
- DNA profile
- Name and residential address
- Name and residential telephone number

- Business Contact Information (BCI) is excluded from the applicability of the PDPA.

- BCI refers to an individual’s name, position name or title, business telephone number, business address, business electronic mail address or business fax number and any other similar information about the individual, not provided by the individual solely for his/her personal purposes.

Best Practice Standards

- Prepare and regularly maintain an inventory map. It should include:
  - What personal data is collected and why
  - Who collects it
  - Where it is stored
  - Who it is disclosed to

- Personal data should only be collected, used or disclosed for
purposes consented to by relevant individuals.

- Data collection form should indicate fields that are compulsory and those that are optional.

- Where verbal consent is given, organisation should subsequently contact the individual and confirm his consent in writing.

- Where personal data is to be \textit{collected} without consent of individual, organisation should first refer to the Second Schedule and ensure that it is permitted to do so.

- Where personal data is to be \textit{used} without consent of individual, organisation should first refer to the Third Schedule and ensure that it is permitted to do so.

- Where personal data is to be \textit{disclosed} without consent of individual, organisation should first refer to the Fourth Schedule and ensure that it is permitted to do so.

- Where a data intermediary is involved, organisation should ensure that the intermediary engaged complies with the PDPA obligations.

- A withdrawal of consent procedure should be implemented, including applicable timeframes, for which notice to withdraw consent can be served by an individual and processed by the organisation. The organisation must inform the individual of the likely consequences of withdrawal of consent, and should allow the individual to withdraw consent thereafter.
4. Access & Correction Obligation

Best Practice Standards

- Organisation should establish a procedure to handle requests for access and correction of personal data.

- Organisation should establish a procedure to send corrected personal data to third parties to which the personal data was disclosed in the last year.

- List of third party organisations to which personal data has been disclosed should be prepared and maintained. List should also include purpose of disclosure.

- A fee structure to defray costs of accommodating such requests should be developed and made available to the individual at the time of his request.

- Where request for access or correction is not to be acceded with, organisation should first refer to S21(3), the Fifth and Sixth Schedules to ensure that it is permitted to do so.
5. Accuracy Obligation

**Reasonable effort** must be taken to ensure accuracy and completeness of personal data where it is likely to be used to make a decision affecting the individual, or to be disclosed to another organisation.

**Illustration of reasonable effort**

- Effort required of organisation depends on circumstances at hand, and factors to be considered include:
  - Nature of personal data and its significance to individual
  - Purpose collected, used or disclosed
  - Reliability of personal data
  - Currency of personal data
  - Impact on individual concerned

**Best Practice Standards**

- Reasonable effort must be taken to ensure that:
  - Personal data collected is accurately recorded
  - Personal data collected includes all relevant parts
  - Appropriate steps are taken to ensure accuracy and correctness of personal data

- Where personal data is collected from a third party source, confirmation should be obtained from the source that accuracy and completeness of personal data has been verified.

- To minimise errors in deciphering handwritten forms, switch to using computerised means such as electronic forms on computers or tablets.
6. Protection Obligation

Illustration of reasonable security arrangements

- **Administrative measures**
  - Conduct training sessions on personal data protection initiatives.
  - Ensure that all employees adhere to the personal data policy of the organisation.

- **Physical measures**
  - Provide personal data access only to authorised personnel on a “need to know” basis.
  - Ensure that computers containing personal data are locked when not in use.

- **Technical measures**
  - Ensure that computer systems are up-to-date and well-protected from system breaches and hacking.
    - Install anti-virus, anti-spyware and personal firewall software on computer systems, and ensuring that scans are performed regularly.
    - Maintain a strong password for electronic files.
      - Change the password periodically.
      - Limit the number of failed logins.
      - Hide password characters when keying in.

**Best Practice Standards**

- Ensure that physical copies of personal data are securely locked up with controls in place. Request for access must be justified and granted only to authorised personnel.

- Keep a record of who has accessed the personal data, including how and when the personal data was used.

---

*Reasonable* security arrangements need to be in place to protect personal data.

---

3 Refer to section 17.5 of the Advisory Guidelines on Key Concepts in the PDPA, page 86 for further examples.
• Schedule regular meetings and audits to keep tabs on personal data protection processes, bearing in mind:
  o The size of the organisation and type of personal data stored
  o Who has access to the personal data
• Whether third parties have access to the personal data
• Ensure that in all outsourced contractual agreements with data intermediaries recognised under the PDPA, there are safeguards in place to protect personal data.

\(^4\) Refer to Appendix 1 for what constitutes data intermediaries and the relevant obligations
7. Retention Limitation Obligation

The organisation must **destroy personal data or remove identifying information of the individual** when
- the **purpose** for initially collecting the personal data is no longer necessary, and
- there is **no legal or business purpose** in retaining the personal data.

**Illustration of ceasing to retain personal data**
- Destroy physical and electronic personal data completely when no longer in use. For example, archiving personal data does not constitute destruction.

**Best Practice Standards**
- Set out a personal data retention policy
  - Specifying varying retention periods for different types of personal data.
  - Including reasons for holding personal data for specific periods.
- Implement a standard operating procedure for destruction of personal data. For example, shredding the personal data before disposal etc.
- Send electronic storage devices for proper destruction and disposal.
  - Use specific software to overwrite files containing personal data.
  - Use specialised hardware such as degausser machines to destroy magnetically recorded personal data.
- Promptly destroy uncollected printouts and faxes containing personal data.
• Ensure that data intermediaries\textsuperscript{5} comply with the PDPA:
  o Review the contract with data intermediaries and ensure that they destroy personal data in accordance with the organisation policy.

\textsuperscript{5} Refer to Appendix 1 for what constitutes data intermediaries and the relevant obligations
8. Transfer Limitation Obligation

Best Practice Standards

- The standard of protection should be legally binding and contain appropriate safeguards.\(^6\)

- In contractual agreements or binding corporate rules\(^7\) with overseas organisations, the obligation to ensure personal data protection should be included.\(^8\)

- Protection should be made with regard to the purpose of collection, use and disclosure by recipient, accuracy, protection, retention limitation, policies on personal data protection, access and correction.\(^9\)

---

\(^6\) According to the Public Consultation Paper on the Proposed Regulations on Personal Data Protection in Singapore, page 11

\(^7\) Internal rules which are legally enforceable and applicable to every organisation

\(^8\) In accordance with the Public Consultation Paper on the Proposed Regulations on Personal Data Protection in Singapore, pages 13-14

\(^9\) As listed in the table on page 97 of the Advisory Guidelines on Key Concepts in the PDPA
9. The Openness Obligation

Best Practice Standards

- Contact information of the data protection officer should be made readily accessible and operational during Singapore business hours.
- The data protection officer should be sufficiently equipped to answer any questions pertaining to the collection, use or disclosure of personal data collected by the organisation.
- The data protection officer should subscribe to the DPO newsletter to be kept updated on the efforts of the PDPC. 10
- The duties of the data protection officer include
  - Implementing measures to tackle and handle complaints received
  - Communicating the organisation’s personal data protection policy to all employees
- Employees should be aware of whom to direct queries to regarding personal data protection.
- Conduct training sessions to inform all employees of the organisation’s data protection policies and their roles in safeguarding personal data.
  - These sessions should be conducted at briefings or employee orientation to allow employees to clarify any doubt and increase their understanding of the responsibilities involved.

Appoint at least one individual in the organisation to be the data protection officer who is in charge of ensuring that the organisation is in compliance with the PDPA. The contact information of that individual should be made available to the public. Personal data protection policies including the complaint process should be made available to the public.

10 Refer to the list of resources below for resources such as the DPO newsletter and PDP toolkit in dual languages.
o Ensure that top management are also aware of their obligations.

• Formulate a compliance manual to assist employees in abiding with the PDPA.
do not call provisions

(DNC) provisions
The Do-Not-Call Obligation

Illustration of the Do-Not-Call Registry

- Ensure that all numbers in the marketing list have given clear and unambiguous consent to receiving telemarketing calls.
  - If no such consent is provided, the DNC Register should be checked to confirm that the number is not listed.

Best Practice Standards

- Develop an internal process to regularly check the DNC Register.
  - Check against DNC registry within 30 days before telemarketing unless there is evidence of clear and unambiguous consent.
- Limit telemarketing activities to existing customers.
- Include information identifying the sender and do not conceal the calling line identity.
- If telemarketing calls are outsourced to third parties, ensure that they comply with the requirements of your organisation’s policy and as set out in the PDPA.
  - Within the contractual agreement with third parties, include the obligation to adhere to your organisation’s personal data protection policy.
1. Is message sent or received in Singapore?
   - yes
   - no

2. Is message a 'specified message'?
   - yes
   - no

3. Is there valid consent from recipient that is clear & unambiguous?
   - no
   - yes

4. Is recipient registered on the DNC register?
   - yes

   DNC provisions do not apply

   no

5. Is sender identity and contact information included?
   - yes

   Message complies with DNC provisions if sent within 30 days of DNC registry check

   no

   Message fails to comply with DNC provisions
Appendix 1

Dealing with Data Intermediaries

What they are

- Data intermediaries are organisations engaged to process personal data for another organisation, not including an employee of the other organisation.

For data intermediaries

- If your organisation is a data intermediary, only obligations 6 and 7 on protection and retention limitation would apply.

- However, you are still responsible for complying with all obligations in other aspects which does not include the scope of a data intermediary.

For organisations engaging data intermediaries

- If your organisation engages data intermediaries, all obligations 1 to 9 will be relevant and must be adhered to.

- Ensure that data intermediaries comply with obligations 6 and 7.

Appendix 2

Employment Best Practices

Relevance of the PDPA in relation to employees’ personal data

1. Appoint an individual within your organisation to be the data protection officer.

2. The data protection officer should be well-informed of his or her roles in protecting the personal data of employees.

3. All employees should be asked to consent to allow the organisation to collect, use and disclose personal data of employees.

4. If personal data of other individuals are to be disclosed to the organisation, those individuals must have consented, ie personal data of family members.
5. The personal data of employees should only be accessed by authorised personnel. Request for access must be justified.

6. Employees’ personal data should not be disclosed to third parties.
   a. If the disclosure to a third party is necessary, ensure that the third party has signed a non-disclosure agreement of the personal data.

7. All employees should keep the data protection officer updated if there are any changes to their personal data, and are responsible for ensuring that the personal data is complete and accurate.

8. Regularly review personal data and ensure timely destruction of personal data that is no longer necessary.
   a. Employ proper methods of disposing employees’ personal data.
List of Resources

1. Personal Data Protection Act 2012
   http://statutes.agc.gov.sg/aol/search/display/view.w3p?page=0;query=DocId%3Aea8b8b45-51b8-48cf-83bf-81d01478e50b%20Depth%3A0%20Status%3Ainforce;rec=0
4. Personal Data Protection Commission Singapore, Public Consultation paper on the ‘Proposed Regulations on Personal Data Protection in Singapore’, (5 February 2013) http://statutes.agc.gov.sg/aol/search/display/view.w3p;ident=b3fc0dc4-a0cb-4796-a91b-475957c03706;page=0;query=DocId%3A8f282d86-5239-4511-9373-3039b3dcb798%20Depth%3A0%20Status%3Ainforce;rec=0
11. DPO Connect Newsletter https://www.pdpc.gov.sg/resources/dpo-connect
The Drew & Napier TMT Team

Lim Chong Kin, Director, Head (Telecoms, Media & Technology)

Chong Kin heads Drew & Napier’s TMT Law Practice Group, which is consistently ranked as the leading IT, telecoms, broadcasting and multimedia legal practice in Singapore.

Chong Kin’s client base spans the entire spectrum in the TMT sector, ranging from the regulators to industry players including global telecommunication carriers, service providers, network operators, hardware manufacturers, equipment suppliers, leading global broadcasters and content providers.

Chong Kin is highly regarded by his peers as well as clients. He has received many recommendations from major publications. Chambers Asia 2015 considers Chong Kin a leading individual and has ranked him in Band 1 for TMT for eight consecutive years, describing him as “an outstanding lawyer who is savvy, intelligent and quick, and possesses excellent business judgement”. Asia Pacific Legal 500 2015/2016 recommends Chong Kin for his expertise in telecommunications, media and technology. The International Who’s Who of Regulatory Communications Lawyers 2008 – 2013 and Who’s Who Legal: Telecoms 2014 recognise Chong Kin for his excellence in telecommunications work. Practical Law Company’s Which Lawyer? lists Chong Kin as a recommended lawyer in the area of telecoms/media.

Tel: +65 6531 4110 • Fax: +65 6535 4864 • Email: chongkin.lim@drewnapier.com

Charmian Aw, Director

Charmian is a Director in the TMT & Data Protection Practice Groups in Drew & Napier.

She is frequently involved in advising companies, particularly in the infocomms, technology and media sectors, on a range of corporate, regulatory, and employment issues in Singapore.

Charmian also has experience in general corporate work, including drafting of agreements and restructuring work involving both private and public listed entities.

More recently, Charmian has been involved in advising and assisting companies on Singapore personal data protection law issues, including reviewing contractual agreements and policies, conducting trainings and advising on audits for data protection compliance and enforceability issues under the Personal Data Protection Act.

Asia Pacific Legal 500 2015/2016 recommends Charmian for her corporate-related TMT and data privacy work.

Tel: +65 6531 2235 • Fax: +65 6535 4864 • Email: charmian.aw@drewnapier.com