# Why You May Need a Privacy Policy

The Personal Data Protection Act ("PDPA") requires a law practice to develop and implement policies and practices that are necessary for the law practice to meet its obligations under the PDPA. Information about these policies and practices are to be made available to individuals on request.

These policies and practices can be set out in a Data Protection Policy, also referred to as a Privacy Policy. A Privacy Policy may be in the form of a physical document, or on your law practice's website, or some other manner.[1]

This article focuses on the Privacy Policy and we provide suggestions on how to develop a Privacy Policy for your law practice.

## Understanding Your Obligations under the PDPA

In order to develop a Privacy Policy, it is important to first understand what your obligations are.

Your law practice's obligations under the PDPA include the following:

1. To be responsible for personal data in its possession or under its control.

2. To collect, use and disclose personal data in accordance with the PDPA.

3. To designate one or more individuals to be responsible for ensuring the law practice's compliance with the PDPA. (Data Protection Officer.)

4. To make available the business contact information of a person who is able to answer questions on behalf of the law practice relating to the collection, use or disclosure of personal data. (The Data Protection Officer may undertake this role.)

5. To develop a process to receive and respond to complaints that may arise with respect to the application of the PDPA. Information about the complaint process to be made available on request.

6. To communicate to staff information about the law practice's policies and practices.

The PDPA provides a number of exceptions and limitations to the various data protection provisions.

It is important to familiarise yourself with the:

1. Personal Data Protection Act

2. Personal Data Protection Regulations

3. Advisory guidelines and guides issued by the Personal Data Protection Commission (PDPC) <https://www.pdpc.gov.sg/>

This article sets out only an overview of the obligations under the PDPA:

### *Appoint a Data Protection Officer*

You[2] must designate one or more individuals to be responsible for ensuring your law practice's compliance with the PDPA. This individual(s), known as the Data Protection Officer (DPO), will be responsible for ensuring that your law practice complies with the PDPA. At least one DPO's business contact information must be made available to the public. The business contact information may be a general telephone or email address of your law practice.

### *Collection, Use and Disclosure of Personal Data*

***Consent*** – You must obtain the consent of the individual before collecting, using or disclosing his or her personal data. (There are exceptions to the consent obligation set out in the PDPA, including if it is specifically required/authorised under the PDPA or any other written law.)

***Purpose*** – You may collect, use or disclose personal data about an individual only for purposes that a reasonable person would consider appropriate.

***Notification of purpose*** – You must notify the individual of the purpose(s) for which you intend to collect, use or disclose the individual's personal data.

You may choose to notify individuals of the purposes for which you collect, use and disclose personal data through your Privacy Policy. This notification is an important aspect of obtaining consent. For an individual to give consent, he or she must first be notified of the purposes for which his or her personal data will be collected, used or disclosed.

You must allow an individual who has previously given consent for collection, use or disclosure of his or her personal data, to withdraw such consent by giving reasonable notice. Upon receipt of a notice to withdraw consent, you must not prohibit the withdrawal of consent, and you must inform the individual of the likely consequences of withdrawing consent.

### *Access to and Correction of Personal Data*

An individual may make a request:

1. for access to his or her personal data;

2. for information about the ways in which the personal data may have been used or disclosed during the past year; and

3. to correct an error or omission in his or her personal data.

You must respond to an individual's request for his or her personal data, or to correct his or her personal data. You should develop a process to receive and respond to such requests.

You must respond to an access request as soon as reasonably possible from the time the access request is received. You should exercise due diligence and adopt appropriate measures to verify an individual's identity, before responding to an access request.

If you are unable to respond to an access request within 30 days after receiving the request, you should inform the individual in writing within 30 days of the time by which you will be able to respond to the request.

Upon receipt of a request to correct an error or omission in the individual's personal data, you must consider whether the correction should be made. Unless you are satisfied on reasonable grounds that the correction should not be made, you should correct the personal data as soon as practicable. If you are unable to correct the personal data within 30 days from the time the request is made, you must inform the individual in writing within 30 days of the time by which you will be able to correct the personal data.

### *Care of Personal Data*

***Accuracy*** – You must make a reasonable effort to ensure that personal data collected by or on behalf of the law practice is accurate and complete if the personal data is likely to be used by you to make a decision that affects the individual concerned or disclosed by you to another organisation.

***Protection*** – You must protect personal data in your possession or under your control by making reasonable security arrangements to prevent unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks.

Security arrangements may take various forms such as administrative measures *(e.g. employees to be bound by confidentiality obligations, training for staff on good practices in handling data),* physical measures *(e.g. storing confidential documents in locked file cabinet systems)*, technical measures *(e.g. installing computer security software, encrypting personal data to prevent unauthorised access, updating computer security and IT equipment)* or a combination of these.

***Retention*** – You must cease to retain documents containing personal data, or remove the means by which the personal data can be associated with particular individuals (e.g. anonymization) as soon as it is reasonable to assume that:

1. the purpose for which the personal data was collected is no longer being served by retention of the personal data; and
2. retention is no longer necessary for any legal or business purposes.

***Transfer*** – You must not transfer personal data to a country or territory outside Singapore except in accordance with the requirements prescribed under the PDPA. You must take appropriate steps to ensure that the recipient is bound by legally enforceable obligations to provide to the personal data transferred a standard of protection that is comparable to that under the PDPA.

## Developing a Privacy Policy

In PDPC's *A Guide to Notification,*[3] PDPC has given examples of the layout of a Privacy Policy. PDPC

recommends the use of simple language, and the use of headers for each section for clarity, e.g. "What types of personal data will be collected?", "How will the personal data be used?". For a web-based Privacy Policy, hyperlinks can be used to provide an overview and allow readers to directly access specific content.

Taking into account your obligations under the PDPA, the following are suggested aspects you could consider including, explaining or expanding on in your Privacy Policy:

1. That the policy applies to all personal data provided to you.

2. The business contact information of your DPO.

3. The types of personal data collected.

4. The purpose of collecting personal data. This may include the following:

    a. For providing the individual with the service they have requested

    b. To prepare legal documents

    c. For billing purposes

    d. To comply with legal and regulatory requirements – (i) conflict checks to prevent conflict of interests; (ii) client due diligence in accordance with the prevention of money laundering and financing of terrorism requirements

5. If the personal data is required for any other purpose, you will notify them and obtain their consent.

6. That you may be required to share information with third parties whether in Singapore or outside of Singapore - this may include e-mail messaging services, delivery & courier services, cloud computing services, services for handling payment transactions.

7. That individuals may access or correct their personal data. Explain the process for doing so, e.g. they could send their request by e-mail or letter to your DPO. If it is not possible to respond within 30 days, you will inform them of the time by which you will respond.

8. That individuals may withdraw consent for the use and/or disclosure of the personal data at any time. Explain the process for doing so, e.g. they could send their request by e-mail or letter to your DPO. Explain the consequences of withdrawing consent, e.g. it may not be possible for you continue to provide services or fulfil the scope of your engagement.

9. That individuals may direct any queries relating to the collection, use or disclosure of their personal data to the DPO.

10. That individuals should update you of any change in their personal data initially provided to you.

11. That you have in place reasonable security arrangements to ensure that the personal data is adequately protected, and is protected against unauthorised or unintended use, access or disclosure.

12. That you will ensure that the personal data is destroyed or anonymized as soon as it is reasonable to assume that (i)) the purpose for which the personal data was collected is no longer being served by the retention of such personal data; (ii) retention is no longer necessary for any business or legal purposes.

13. That if personal data is to be transferred out of Singapore, you will comply with the PDPA in doing so – this includes obtaining the individual's consent unless an exception under the PDPA or law applies.

14. That if individuals have a complaint about how you are handling their personal data or are complying with the PDPA, they can submit a complaint. Explain the process for doing so, e.g. they could send their complaint by e-mail or letter to your DPO.

**Knowledge Management Department**
The Law Society of Singapore

**Notes**

1 The following is stated in the 'Advisory Guidelines on Key Concepts in the Personal Data Protection Act' issued by the Personal Data Protection Commission:

14.12 "The PDPA requires organisations to develop and implement policies and procedures that are necessary for the organisation to meet its obligations under the PDPA. In addition, organisations are required to make information available on such policies and procedures. Organisations may wish to develop a Data Protection Policy (also referred to as a Privacy Policy) to set out its policies and procedures for complying with the PDPA. An organisation may choose to notify individuals of the purposes for which it collects, uses and discloses personal data through its Data Protection Policy."

14.13 "(a) Where the policy is not made available to an individual as a physical document, the organisation should provide the individual with an opportunity to view its Data Protection Policy before collecting the individual's personal data. …. "

2 "You" in this article refers to your law practice.

3 <https://www.pdpc.gov.sg/docs/default-source/other-guides/a-guide-to-notification-v1-0-(110914).pdf?sfvrsn=8>