PAM

PRACTICE NOTE

AN INTRODUCTION TO THE PERSONAL DATA PROTECTION ACT 2010 (ACT 709) [PDPA] FOR ARCHITECTS

a publication of

PAM™

NOVEMBER 2024

SERIAL NO: **PN** 2024-5

ACTS/PDPA

Practice Note: An Introduction to the Personal Data Protection Act 2010 (Act 709) [PDPA] for Architects

Introduction

The Personal Data Protection Act [PDPA] 2010 (Act 709) is to regulate the processing of personal data with respect to commercial transactions and to safeguard the interests of data subjects (individuals with personal information that will form the basis of data collected).

The PDPA was passed in May 2010 and received Royal Assent in June 2010. It became operational on November 15, 2013. Together with the PDPA, subsidiary legislation, also enforced on November 15, 2013, encompassed issues such as the appointment of the Personal Data Protection Commissioner (PDPC), registration of data controllers and fees that may be imposed under the PDPA.[1]

A data controller is any person who processes, has control over or authorizes the processing of any personal data with respect to commercial transactions.

Other legislation includes the Personal Data Protection Regulations,[2] which allow the authorities to supervise and monitor data controllers' compliance with the law, and the Personal Data Protection Standard 2015,[3] which establishes certain security standards for personal data processed electronically.

Processing of Personal Data

Under the Act, "processing" refers to the collecting, recording, holding or storing of personal data or carrying out any operation or set of operations on the personal data. Examples of the processing of data are as follows:

- Collecting data through forms, by phone, or via the web;
- Publishing data;
- Selling data;
- Using administrative data;
- Using data for marketing purposes;
- Recording data;
- Disclosing or providing data to other organizations; and / or
- Destroying data.

Complying with the Personal Data Protection Principles

The processing of personal data by a data controller needs to comply with the following seven (7) fundamental principles, namely:

i. the General Principle;
a controller is not allowed to process another person's personal data without their consent. The term process here should be understood as handling data through automated or computerized means or methods or any other process;

ii. the Notice and Choice Principle;
prior information and purposes are communicated to the data subject concerned;

iii. the Disclosure Principle;
disclosure of the purpose of a subject's personal data in order to identify the purpose for which the personal data is to be disclosed;

Notes:

[1] An amendment to the Personal Data Protection Act 2010, cited as the Personal Data Protection (Amendment) Act 2024 is awaiting gazette by Parliament. Architects should keep abreast of the changes to the act. The PDPA 2010 can be downloaded via https://www.pdp.gov.my/ppdpv1/en/akta/pdp-act-2010

[2] The PDP Regulations can be viewed at https://www.pdp.gov.my/ppdpv1/en/akta/personal-data-protection-regulations-2013/.

[3] The PDP Standard 2015 can be viewed at https://www.pdp.gov.my/ppdpv1/en/akta/personal-data-protection-standard-2015/

iv. the Security Principle;
when processing any subject's personal data, take steps to ensure that the data is secure, not modified, misused or given to unauthorized parties;

v. the Retention Principle;
personal data is not allowed to be stored in a processing for more than the necessary time limit;

vi. the Data Integrity Principle;
ensure personal data is accurate, complete, not confusing and up-to-date in accordance with the purpose for which the data is stored and processed;

vii. the Access Principle.
a person should be given the right to access his personal data held by a data controller and also be able to correct his data so that it is up-to-date

Under the Act, failure to comply with any of the seven (7) principles will attract a fine not exceeding RM300,000, imprisonment not exceeding two years, or both.

Guidelines or Standards issued on the Compliance of the Seven (7) Principles

The principles that are commonly breached are the *(i) General, (iv) Security, (v) Retention and (iii) Disclosure principles*. These are probably caused by the concerns of having to bear the costs of compliance with the principles as well as the lack of awareness of the public or businesses towards personal data protection in Malaysia.

The Personal Data Protection Standard 2015 (**"Standard 2015"**) established the following three (3) minimum mandatory standards that entities must strictly adhere to:

- the Security Standard;
- the Retention Standard; and
- the Data Integrity Standard.

Security Standard
In processing a data subject's personal data, a data controller or processor is required to undertake all reasonable and practicable steps to prevent any loss, misuse, modification, unauthorized or accidental access, disclosure, alteration or destruction of the said data. Where the data processing is carried out by an external third party, the data controller must secure sufficient guarantees from the third party service provider in respect of its security measures for the protection of the data and undertake all reasonable steps to ensure compliance with this principle.

Retention Standard
This standard stipulates that a data subject's personal data must not be retained longer than necessary for the fulfillment of the purpose for which it is being processed. Upon fulfillment of the said purpose, it is the duty of the data controller to take all reasonable steps to destroy or permanently delete all personal data after the retention period. The retention periods are varied in accordance with the requirements set out by different laws; for instance, data regarding employee payrolls are required to be kept for seven (7) years. On the other hand, if the data does not hold any legal value, it shall be disposed of within 14 days, while inactive, personal data shall be disposed of within 24 months.

Data Integrity Standard
This standard imposes a continuous obligation upon data controllers to take reasonable steps to ensure that the personal data is accurate, complete, not misleading and kept up-to-date with regards to the purpose for which the personal data was collected and further processed.

While the above are some of the minimum standards that the PDPC has prescribed to assist data controllers and businesses in working towards compliance with the above-mentioned three (3) data standards which are commonly breached, it is still mandatory to comply with the remaining principles of the seven (7) data principles as prescribed by the Act. If a commercial organization fails to comply with both

- the requirements under the Standard 2015; and
- the principles under the Act,

it and/or its officers will be liable for penalties and/or imprisonment under both.

Main Classes of Data Users

There are 13 categories of data controllers that are required to register with the Personal Data Protection Commissioner. Architecture is under the list of 'Services' which require registration and the following are the type of firms that are required to register:

- A private company, as defined in Section 4 of the Companies Act 1965 [Act 125];
- A partnership as defined in Section 3 of the Partnership Act 1961 [Act 135];
- Sole proprietors of a business registered under the Registration of Business Act 1956 [Act 197][4]

How To Register

Go to the link at daftar.pdp.gov.my and complete the registration.

Registration fees and Annual Renewal

Sole proprietor - RM 100.
Partnership - RM 200.
Private company - RM 300.
Public company - RM 400.

Penalties

Failure to register is an offence punishable with a fine of up to RM500,000, up to three years' jail, or both.

A breach of the PDPA may result in an inquiry or investigation by the Commissioner (either on its own initiative or based on a complaint received). If, following the investigation, the Commissioner decides that the PDPA has been contravened, the Commissioner may serve an enforcement notice specifying, inter alia, the breach, the steps required to be taken to remedy the breach within a certain period and directing the relevant data controller if necessary, to cease processing the personal data. Fines of up to RM200,000, two years' imprisonment, or both are possible for failure to comply with the Commissioner's enforcement notice.

The Commissioner may also revoke the registration of a data controller in certain circumstances; for example, if the data controller has failed to comply with the provisions of the PDPA or with any conditions imposed as part of the registration. *If an architectural practice commits an offence, its principal, partners or directors, may be charged severally or jointly for non-compliance by the practice, subject to certain limited defenses.*

Notes:

[4] The Act is silent on whether sole proprietorships registered with Lembaga Akitek Malaysia need to register as data controllers. Notwithstanding the above, sole proprietorships should ensure that their practices comply with the Personal Data Protection Standard 2015 to avoid any issues with the authorities.

Steps to Take to Ensure Compliance with the Minimum Standards

The following are some of the steps to take to meet the minimum standards of data protection:

a) Security Principle

DO's	DON'Ts
Access control is well-established and safeguarded.	Documents containing personal data are placed at inappropriate, unsecured or publicly accessed locations.
ID and Password management are well-established, maintained and secured.	Documents are exposed and not properly kept and retained.
Documents are kept in secure locations and databases.	Malfunctioning CCTVs and delays in remedying the same resulting in further data or financial losses.
	Documents are not properly disposed off or destroyed.
	Passwords to the computer log-in system are exposed and shared with colleagues.

b) Retention Principle

DO's	DON'Ts
All documents containing personal data are stored in a secure location.	Improper storage of business contracts, customer and supplier data, and financial records or documents.
An effective procedure for unused records and data disposal is well established and adhered to.	Improper or careless use of storage cabinets or facilities.
	Lack of an effective policy on data retention and disposal.
	Cabinets used to store items other than documents.

c) Data Integrity Principle

DO's	DON'Ts
To prepare a form for data subjects to update personal data online or via a physical copy.	Possession or retention of obsolete or misleading personal data.
To update, correct or amend personal data immediately upon receiving a personal data correction notice from the data subjects.	Data is tampered by hackers or anonymous scammers.
To ensure that all relevant legal requirements are fulfilled by identifying the types of data or documents that are required to support or verify the authenticity of the personal data of the data subjects.	The updated and uploaded information is false or inaccurate.
To inform the data subjects about the procedure and ways of updating their personal data, either through an online portal or by displaying an announcement or notice on the data user's premises, and by other appropriate methods of notification or alert.	

Conclusion

Apart from being aware of how the PDPA and its regulations may affect them, all Architects should also be aware that the situation is nevertheless, very fluid; at the time of writing of this PN, it must be noted that further Guidelines are currently being developed by the Personal Data Protection Officers. Architects as such, should continue to be aware of any new developments that may arise within this sphere.

Regardless of the existence and application of the minimum standards, it is mandatory for data users or any companies processing personal data to abide by the seven (7) principles stipulated under the Act. Any principal who has concerns as to whether his/her business operations, including data processing and retention, are in compliance with the principles of the Act and the above minimum standards is advised to seek legal advice accordingly.

PRACTICE NOTE | PN 2024-5
This Practice Note was authored/collated primarily by Ar. Au Tai Yeow, reviewed by Practice Note Working Group, Professional Practice Committee 2024-25 and issued on 8 November 2024.