Paradigm®

INTERNATIONAL SOCIETY OF PRIMERUS LAW FIRMS

FALL 2018

President's Podium: Serving Our Communities

In-House Lawyers Find Value with Primerus

Six Diamonds: Primerus Firms Sparkle for Clients Around the World

Current Legal Topics:

Asia Pacific

Europe, Middle East & Africa

Latin America & Caribbean

North America

Personal Data Protection in Malaysia

The Malaysia Personal Data Protection Act 2010 (PDPA 2010) was enacted and came into effect on June 10, 2010, to protect the rights of anyone who shares or provides personal information to an organization (data subjects). In short, PDPA 2010 governs the relationship between the data user/data processor and the data subject. Under PDPA 2010, a data user/data processor is defined as a person or organization who processes the data. Section 2 of the PDPA provides that it is applicable to a person who processes, controls or authorizes the processing of any personal data in respect of commercial transaction. Under Section 4 of the PDPA 2010, personal data is defined as any information in commercial transactions that relates directly or indirectly to a data subject/individual.

Izzat Emir Hakimi Bin Jasme

Izzat Emir Hakimi Bin Jasme is a corporate lawyer at J. Lee & Associates. He practices in the area of Islamic finance, mainly in drafting Islamic transaction documents for several banks with Islamic financing facilities throughout Malaysia.

J. Lee & Associates
A-16-13, Tower A
No.5 Jalan Bangsar Utama 1
Kuala Lumpur 59000
Malaysia

+60 3 2288 1699 Phone

jlee@jlee-associates.com
jlee-associates.com

Requirements Under PDPA 2010[1]

PDPA 2010 embraces the following principles:

1. General Principle[2]

Consent is the backbone of this principle. Generally, a data user cannot process personal data about the subject without his or her consent.[3] This means that if the data subject or anyone subscribes to the data provider, then the data provider must get the consent from the data subject first. However, the law does provide certain exceptions[4] where consents are not necessary. The exceptions are described under section 6 (a) to 6 (f) of the PDPA 2010.

2. Notice and Choice Principle[5]

In addition, the data user must also comply with the Notice and Choice Principle. Under this principle, notice is the elemental backbone. A data user must inform the data subject by written notice as outlined in Section 7 of the PDPA 2010 on several matters, such as the purpose for which the personal data is being used. The notice must be given as soon as practical as stated in Section 7(2) of the PDPA 2010. The notice must be either in Malay or English, and the data subject must be given clear and readily accessible means to exercise his choice.[6]

3. Disclosure Principle[7]

Subject to Section 39 of the PDPA 2010, personal data cannot be disclosed for any purpose other than the purpose for which the personal data was to be disclosed at the time of its collection. Furthermore, personal data cannot be disclosed for any other purpose than the one directly related to the purpose aforementioned.[8] Personal data also cannot be disclosed to any party other than a third party of the class of third parties under PDPA 2010.[9]

4. Security Principle[10]

The security principle addresses the responsibility of the data user to take care of the personal data of the data subject. A data user must take practical steps to protect the personal data from any loss, misuse, modification, unauthorized or accidental access or disclosure, alteration or destruction. The data user shall also ensure that the data processor provides sufficient guarantees in respect to the technical and organizational security measures on how the data processing is to be carried out and take reasonable steps to ensure compliance with those measures.[11]

5. Retention Principle

PDPA 2010 provides that the personal data processed for any purpose shall not be kept longer than is necessary for the fulfilment of that purpose.[12] Also, when the personal data is no longer required for the purpose for which it was to be processed, the data user shall take every reasonable step to ensure that all personal data is destroyed or permanently deleted.[13]

6. Data Integrity Principle[14]

Under this principle, a data user shall take reasonable steps to ensure that the personal data is accurate, complete, up-to-date and not misleading by having regard to the purpose, including any directly related purpose, for which the personal data was collected and further processed.

7. Access Principle[15]

This principle requires that a data subject shall be given access to his personal data held by a data user and he must be able

to correct that personal data where the personal data is inaccurate, incomplete, misleading or not up-to-date, except where compliance with a request to such access or correction is refused under this Act.

Non-Compliance with the PDPA 2010

Non-compliance by a data user of any of the principles constitutes an offense under the PDPA and is liable to a fine not exceeding 300,000 Ringgit Malaysia (RM300,000.00) or imprisonment for a term not exceeding two years or both.[16]

Malaysia's PDPA 2010 and European Union's Global Data Protection Regulation

The main difference between these two laws is the interpretation of the word "personal data," where under Global Data Protection Regulation (GDPR) it is described as any information relating to an identified or identifiable natural person. Meanwhile, PDPA 2010 confines 'personal data' to any information in respect of commercial transactions.[18] The other distinction between the PDPA 2010 and GDPR is on the exemption. PDPA 2010 specifically listed the exemptions under Section 45 of the PDPA 2010, including prevention or detection of crime or for the purpose of investigations, apprehension or prosecution of offenders and the assessment or collection of any tax or duty or any other imposition of a similar nature. Meanwhile, in Chapter 9 of the GDPR, it provides for provisions relating to specific processing situations including freedom of expression, public access to official documents, public interest and processing data in context of employment. PDPA 2010 is only applicable in Malaysia, while GDPR provides protection to European Union (EU) citizens no matter where their data travels.[19] Any company, anywhere, that has a database that includes EU citizens is bound by its rules. The last difference between these two laws is on the penalty imposed. A fine not exceeding 300,000 Ringgit Malaysia (RM300,000.00) or imprisonment for a term not exceeding two years or both will be imposed in case of not complying with PDPA 2010, while breaches to GDPR can cost companies up to 20 million Euros or up to 4 percent of the breacher's annual global turnover.[20]

Conclusion

The enforcement of the PDPA 2010 indicates that Malaysia is serious in protecting personal data. Non-compliance with the principles listed under PDPA 2010 will cause the data provider to face the penalty imposed under the PDPA 2010. Even though the penalty imposed by the PDPA 2010 is far lower than the one imposed by GDPR, Malaysia is on the right track toward protecting the personal data of the data subject. It changes the landscape of data protection in Malaysia, with respect to the confidentiality of the data. P

1 Section 5 of the PDPA 2010
2 Section 6 of the PDPA 2010
3 Section 6(1) of the PDPA 2010
4 Section 6(2) of the PDPA 2010
5 Section 7 of the PDPA 2010
6 Section 7(3) of the PDPA 2010
7 Section 8 of the PDPA 2010
8 Section 8(a) of the PDPA 2010
9 Section 8(b) of the PDPA 2010
10 Section 9 of the PDPA 2010
11 Section 9 (2) (a), (b) of the PDPA 2010
12 Section 10 (1) of the PDPA 2010
13 Section 10 (2) of the PDPA 2010
14 Section 11 of the PDPA 2010
15 Section 12 of the PDPA 2010
16 Section 5(2) of the PDPA 2010
17 Article 4 of the GDPR
18 Section 4 of the PDPA 2010
19 Article 3 of the GDPR
20 Article 83 of the GDPR