AZMI & ASSOCIATES
A member of TerraLex worldwide | advocates & solicitors
We care & share

PRIVACY LAW IN MALAYSIA

Introduction

With the rapid development of technology and the widespread usage of the Internet over the last decade, anyone can have access to almost anything including the personal information of others. Today, the usage of the Internet is no longer confined to connecting people and conducting research, but it has become a platform for many to store information and advertise themselves and their businesses.

Unlike other jurisdictions, Malaysia has no specific law such as a Privacy Act to protect personal privacy, except for the *Personal Data Protection Act 2010* ("***PDPA***"), which deals with personal data and focuses on regulating the processing of 'personal data' in commercial transactions.

Even though there is no principle on the right to privacy in Malaysia, the Federal Court case of ***Sivarasa v Badan Peguam Malaysia & Anor***[1] held that the right to personal liberty under Article 5(1) of the Federal Constitution includes the right to privacy.

What Does "Privacy" in PDPA Entail?

There is no general definition of 'privacy' embedded under the PDPA. However, 'personal data' under Section 4 of the PDPA is defined as any information in respect of commercial transactions which: -

a) is being processed wholly or partly by means of equipment operating automatically in response to instructions given for that purpose;

b) is recorded with the intention that it should wholly or partly be processed by means of such equipment; or

c) is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system.

The information relates directly or indirectly to a data subject, who is identified or identifiable from that information or from other information in the possession of a data user, including any sensitive personal data and expression of opinion about the data subject; but excludes any information that is processed for the purpose of a credit reporting business carried on by a credit reporting agency under the Credit Reporting Agencies Act 2010.

In simpler terms, the aim of the PDPA is to safeguard the personal data of individuals that are collected, stored and used ("data subject") from being abused by the person or persons who have control over the personal data ("data user") or authorises the processing of such personal data ("data processor"). This wide definition covers details such as name, address, contract details and your national registration identity card. It also includes 'sensitive' personal data such as the physical or mental health condition of an individual, their political opinions and even religious beliefs.[2]

A Guide for Data Users

There are seven data protection principles[3] in the PDPA that data users[4] should comply with and they are briefly stated as follows:-

No.	Type of Principle	Method
1.	General	Ask for the data subject's consent before processing their data.
2.	Notice and Choice	Give a written notice to the data subject informing them details such as the description of data, the purpose of the data, the sources, the right to request access and correction and the class of third parties to whom the data may be disclosed to.
3.	Disclosure	Ask for the data subject's consent if the personal data is to be disclosed for any other purpose other than the purpose for which the personal data was to be disclosed at the time of collection or to any party other than the third party notified by the data user.
4.	Security	Take practical steps to protect the personal data from any loss, misuse, modification, unauthorized or accidental access or disclosure, alteration or destruction.
5.	Retention	Ensure that the personal data is not kept longer than necessary and to take all reasonable steps to ensure all personal data is permanently deleted or destroyed if it is no longer required for the purpose it was to be processed.
6.	Data Integrity	Take reasonable steps to ensure the personal data is accurate, complete, not misleading and kept up-to-date.
7.	Access	Give the data subject access to their personal data and be able to correct their inaccurate, incomplete, misleading or not up-to-date personal data.

As per **Section 5(2) of the PDPA**, a data user who fails to comply with these seven principles commits an offence and shall be liable to a fine or to imprisonment or to both upon conviction. Hence, a breach in the data protection can be costly to the data user's business as a data subject may pursue an action against them. Therefore, it is crucial for data users to comply with the abovementioned principles.

Other Statutes

Sections 211 and 233 of the *Communications and Multimedia Act 1998* ("***CMA***") prohibits the provision of offensive content (which is indecent, obscene, false or menacing) with the intent to annoy, abuse, threaten or harass any person. However, these two sections are not specifically about the right to privacy and very broad to describe the offensive content on the internet. Further, it is subject to the court's assessment whether the content falls under the types of offensive content on the internet as provided in Sections 211 and 233 of the CMA.

Under Section 509 of the Penal Code, it is a criminal offence to "intrude upon the privacy" of a person; however this strictly applies to actions which insult the modesty of a person. Upon conviction, an offender may be punished with imprisonment for a term which may extend to five years or with fine or with both.

Conclusion

The Malaysian courts are generally reluctant to accept that there is a general principle of invasion of privacy. However, the courts did in some occasions find that a person's privacy had been intruded, especially where there is a case for breach of confidence (e.g., doctor-patient relationship). With the limited scope of privacy introduced by the PDPA, an individual who wishes to bring an action under the PDPA can only do so when their personal data privacy has been breached, and not for the rights to privacy in general.

As public awareness of privacy rights in Malaysia is still low and this problem is aggravated by the absence of modern legislation penalising invasion of privacy as a whole, it is timely for our lawmakers to come up with our own legislation that provides the protection for all types of privacy (not just the protection of private data) instead of adopting the common law.

---

1. [2010] 3 CLJ 507
2. Section 4 of the PDPA
3. Section 6 to Section 12 of the PDPA
4. Section 5(1) of the PDPA

Prepared by:

Omar Saifuddin Abdul Aziz
Senior Associate 1
omar.saifuddin@azmilaw.com

Demetria Rinesha Samuel
Legal Executive
demetria@azmilaw.com

Nur Amalina Azami
Legal Executive
nuramalina@azmilaw.com

Corporate Communication
Azmi & Associates

2 November 2020