Malaysian Journal of Syariah and Law
مجلة الشريعة والقانون بماليزيا

Vol. 12, No. 1, pp. 135-147 | APRIL 2024
DOI: https://doi.org/10.33102/mjsl.vol12no1.458

DATA BREACHES EXIT STRATEGY: A COMPARATIVE ANALYSIS OF DATA PRIVACY LAWS

[i,*]Nur Adlin Hanisah Shahul Ikram

[i]Ahmad Ibrahim Kulliyyah of Laws (AIKOL), International Islamic University Malaysia (IIUM), PO Box 10, 50728, Kuala Lumpur, Malaysia

*(Corresponding author) e-mail: adlinhanisah92@gmail.com

Article history:
Submission date: 31 Aug 2023
Received in revised form: 25 Oct 2023
Acceptance date: 28 Dec 2023
Available online: 15 April 2024

Keywords:
Personal data, data security, data protection impact assessment, data protection officer, data breach notification

Funding:
This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

Competing interest:
The author(s) have declared that no competing interests exist.

Cite as:
Shahul Ikram, N. A. H. (2024). Data breaches exit strategy: A comparative analysis of data privacy laws. *Malaysian Journal of Syariah and Law*, *12*(1), 135-147. https://doi.org/10.33102/mjsl.vol12no1.458

ABSTRACT

Data has become highly valuable in the era of digitalisation and is the main target of cybercriminals. Cybercriminals steal data by exploiting system vulnerabilities. The rise of catastrophic data breach incidents affects business operations, reputation and legal standing, leading to business disruptions, financial loss and reputation damage. These incidents have raised data security concerns. The frequent incident is partly due to insufficient security measures in place. This article employs doctrinal research focusing on legal principles based on legislation to analyse Malaysia's legal framework for protecting personal data in Malaysia and a comparison with other jurisdictions, i.e. the European Union General Data Protection Regulation (GDPR), the Singapore Personal Data Protection Act 2012 and the China Personal Information Protection Law (PIPL). The findings show that Malaysia's data protection laws fall short of the international norm in some areas. This article suggests that Malaysian policymakers may amend the Personal Data Protection Act 2010 to align with international data protection standards to strengthen data security measures in preventive, detective and responsive data breaches. Consequently, this article provides an analysis of data protection laws in Malaysia and compares them with other advanced jurisdictions. It offers valuable insights into the challenges and opportunities involved in safeguarding personal data, the legal framework, and organisational strategies related to data privacy and security.

Introduction

In the era of digitalisation, one's data can be traced and retrieved abundantly from disparate sources, including devices and applications, and the list goes on. The data ingestion occurs continuously and rapidly. When raw data is combined with the rest of the available data in the database, it reveals its value (Agrawal et al., 2012). This valuable data can reflect a person's spending behaviour and social media patterns, and this dynamic allows the data profiling to change quickly (Beebeejaun, 2019). Data has become one of the most valuable commodities, commanding immense power and influence for businesses (The Economist, 2017).

These valuable data have become the main target of cybercriminals, and they steal data by exploiting the system's vulnerability in the system or network (Agrawal et al., 2012). The vulnerabilities can arise from a lack of security upgrades, weak passwords, lax access controls, phishing attempts, social engineering techniques, or unauthorised access. Organised cybercriminals have become more vigorous, sophisticated, and challenging, making data breaches harder to prevent (Olejarz, 2015). Data breaches are one of the most significant data security issues. Data breach happens when one's data can be seen by people who should not be able to see it. A data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, or unauthorised disclosure of, or access to, personal data (Information Commissioner's Office, n.d.). It can be considered a security incident that compromises the confidentiality, integrity, or accessibility of personal data. Based on the reported cases, stolen data will be used for illicit purposes such as ransom, selling it on the dark web, identity theft, or other fraudulent activities (R. Loheswar, 2022).

The implications of data breaches on data subjects might often be intangible, but they are still real. It includes the risk of future injuries, such as traumatised data breach risk (Solove & Citron, 2018).). Data breaches also cause data users to suffer operational disruptions to their businesses, severe reputational damage, financial loss, and loss of customers and investors' trust and confidence in the long run (Schmittmann & Teng, 2020). Further, there is the possibility that the data users might face hefty fines imposed by the authorities.

Malaysia has been experiencing frequent massive data breaches involving financial institutions, telecommunications, multimedia and broadcast companies, internet providers, government agencies, and more, exposing the data of millions of people (R. Loheswar, 2022). In August 2022, the Malaysian Personal Data Protection Commissioner revealed that roughly 3,699 reported instances of personal data breaches in Malaysia have occurred since 2017 (Kaur, 2022). The Surfshark (a Netherlands cybersecurity company) survey shows Malaysia suffered 44.2 million account breaches from 2004 to 2022 (Shivani Supramani, 2023). The number of compromised accounts exceeded the number of the Malaysian population, around 32.7 million in 2022 (Ministry of Economy Department of Statistics Malaysia, 2022). According to Surfshark's latest study, approximately 660,000 Malaysian accounts were compromised in data breaches, placing Malaysia as the 11th most breached country between April and June 2022 (Fam, 2022). Cybersecurity risks are the primary concern of regulators, including Bank Negara Malaysia (Schmittmann & Teng, 2020).

Data breaches seem inevitable and might happen in just a matter of time. According to a 2022 PwC survey, cybercrime poses the biggest threat to all organisations, followed by customer fraud and asset misappropriation (PwC's Global Economic Crime and Fraud Survey 2022, 2022). Most organisations are still not well prepared or do not understand the risks they are facing. According to the Global Economic Crime Survey 2016, only 37% of organisations have a cyber incident response plan (PwC, 2016). Organisations must find new ways to handle and protect their valuable data (Gaidarski & Kutinchev, 2019).

The Malaysia Personal Data Protection Act 2010 (PDPA 2010) can be used as a benchmark to assess the country's adequacy of data protection law. However, scholars highlighted that the PDPA 2010 has several shortcomings (Alibeigi & Munir, 2020; Islam et al., 2021). Data breaches in Malaysia are rising, showing that current laws are inadequate. Malaysia organisations need robust strategic plans for preventing and managing data breaches by establishing appropriate incident responses and complying with current standards and regulations. Learning from the best practices like the EU GDPR, the Singapore PDPA 2012,

and the China PIPL would be a good solution to strengthen the adequacy and functions of the Malaysia PDPA 2010.

Background of data privacy laws

Different jurisdictions have different approaches to protecting personal data. It is crucial to discuss the background of the Malaysia PDPA 2010, the EU GDPR, the Singapore PDPA 2012 and the China PIPL before discussing how Malaysia can learn best practices from advanced jurisdictions.

The Malaysia Personal Data Protection Act 2010 (PDPA 2010)

Malaysia is the first ASEAN country to draft a data protection regime and pave the way for other ASEAN and Asian nations (Alibeigi & Munir, 2020). The PDPA 2010 is the primary regulation on the processing of personal data, which came into force on 15 November 2013. The main objective of the PDPA 2010 is to protect individuals' data in commercial transactions (section 2). The government and credit reporting agencies are exempted from the application of this Act. This Act consists of seven main principles, i.e. general principle (section 6), notice and choice principle (section 7), disclosure principle (section 8), security principle (section 9), retention principle (section 10), data integrity principle (section 11), and access principle (section 12). In analysing the data security principle under this Act, it should be read together with standards 4 and 5 of the Personal Data Protection Standards 2015. Failure to comply with 7 data principles or breach of the cross-border data restriction is punishable by a fine of up to RM 300,000 or imprisonment for up to two years or both (section 5(2)).

The European Union General Data Protection Regulation

The EU parliament passed the General Data Protection Regulation on 14 April 2016. It came into force on 25 May 2018, replacing the 1995 EU Data Protection Directive 95/46/EC (Recital 171). The European Union's GDPR aims to harmonise data privacy across Europe. The GDPR is in the form of a regulation rather than a directive. The Standard GDPR imposed in the EU has become a new benchmark for other countries to follow. The GDPR imposes strict new rules on controlling and processing data, including introducing the mandatory appointment of a data protection officer (Article 37), a mandatory data breach notification (Article 33), and the extraterritorial scope of the application (Article 3). The regulation has a binding effect on all entities holding and processing EU residents' data regardless of geographic location (Article 3). The GDPR imposes a percentage revenue-based fine. The penalties for lesser offences are €10 million or 2% of annual global turnover. Moreover, the maximum is up to €20 million or 4% of annual worldwide turnover, whichever is higher (Article 83).

The Singapore Personal Data Protection Act 2012 (PDPA 2012)

The Personal Data Protection Act 2012 is Singapore's standard for protecting personal data. The PDPA was passed by the Parliament of Singapore on 15 October 2012 and implemented in three phases. The PDPA 2012 came into force on 2 January 2013. The PDPA 2012 governs the collection, use, disclosure and care of personal data by organisations in Singapore (Section 4). It does not matter whether the organisation collects, process and disclose data for commercial or non-commercial purposes. The term "organisation" includes any individual, company, association or body of persons, corporate or unincorporated, whether or not formed or recognised under the law of Singapore or resident, or having an office or a place of business in Singapore (Section 2). The Act also protects the personal data of individuals who have been dead for ten years or fewer (section 4(4)(b)).

The Personal Data Protection Act 2020 (Amendment Act) (No. 40 of 2020) came into force on 1 February 2021. This Amendment Act seeks to amend the PDPA 2012 to introduce a mandatory requirement for data breach notification (Part 6A), the expansion of the scope of deemed consent (sections 15 and 15A), the inclusion of additional exceptions to express consent, and personal liability for egregious mishandling of personal data. The amendment includes an increase in the maximum financial penalty for breaches of the PDPA. The organisations can be fined up to 10% of their annual turnover in Singapore exceeds SGD 10 million, whichever is higher (section 48J).

The China Personal Information Protection Law (PIPL.)

The Personal Information Protection Law (PIPL) lays down the fundamental framework for personal information protection in the People's Republic of China (PRC). The PIPL was adopted at the 30th meeting of the Standing Committee of the 13th National People's Congress on 20 August 2021 and came into effect on 1 November 2021. The official text is only available in Chinese. This regulation governs how entities or individuals collect, store, use and transfer personal information and addresses data leakage problems. Any organisation or individual determining the purposes and means of processing personal information is a Personal Information Processor or Handler (PI handler). The PIPL has an extraterritorial effect where the regulation also applies to those who process data Chinese citizens' Personal Identifiable Information (PII) outside of China (Article 3). The PIPL imposed more stringent requirements on data transfer and localisation (Chapter III), Personal Information Processors' obligations (Chapter V), providing individual rights in personal information processing activities (Chapter IV), and increased penalties and fines on organisations upon violation are anticipated (Article 66).

China imposed stringent fines and penalties on entities or individuals for violating the PIPL. In a minor violation, the personal information protection authorities may issue an order for rectification, issue warnings and confiscate illegal gains. If they refuse to rectify, they may be subject to a fine of not more than RMB 1 million, and the responsible person in charge may be subject to fines between RMB 10,000 and 100,000. The offending entity's business or related business activities may be suspended pending rectification of the alleged violations, and the entity may be required to report to the relevant authorities regarding such suspension. In the event of grave violations of the PIPL, if they refuse to rectify, offended entities may be fined up to RMB 50 million, or 5% of annual revenue. The person in charge and other personnel who bear direct responsibility will be liable to a fine between RMB 100,000 and RMB 1 million and may be prohibited from holding certain positions, including director, supervisor, high-level manager or personal information protection officers, for a certain period. The personal information protection authorities may also issue an order to suspend the business or operation for rectification and notify authorities in charge of cancellation of business permits or licenses (Article 66). The violation will be recorded and published publicly (Article 67).

Methodology

This article employs doctrinal legal research focusing on legal principles based on legislation to analyse Malaysia's legal framework for protecting personal data in Malaysia, including exit strategy for data breaches. Data for this article were extracted from several literature reviews of primary materials, mainly from statutes, guidelines, administrative rules, and regulations. Secondary materials as a supplement to the primary references were also referred to, such as articles in established journals, textbooks, newspapers, and online sources. This article is a comparative study that aims to learn the best practices from other advanced jurisdictions, i.e. the European Union General Data Protection Regulation, the Singapore Personal Data Protection Act 2012 and the China PIPL.

Data Security

When a thing's value is feared to be threatened or attacked, there is a need for security and to put preventive measures to a related risk (Sonny Zulhuda, 2010). There is a need for data security to protect the valuable data. Data security is the practice or process of protecting data and maintaining its confidentiality, integrity, and availability from unauthorised access, loss or theft throughout its entire lifecycle (Data Security | NCCoE, n.d.). The data security principle is one of the seven main principles under the PDPA. To effectively prevent data breaches, section 9 of the PDPA requires data users to protect data by taking *"practical steps to protect the personal data from any loss, misuse, modification, unauthorised or accidental access or disclosure".* The wording "taking practical steps" broadly defines measures to protect the data. Data users have the liberty, flexibility and suitability of measures to put in place to tighten their data security features, access, storage and recovery. Section 9 of the PDPA is almost similar to Article 9 of the China PIPL, where the PI handler is responsible for taking necessary measures to ensure the security of the personal information they process. Adopting Article 25(1) of the GDPR, the Data Protection by Design approach would be most helpful by incorporating data privacy features into the design, systems, and processes. It is crucial to incorporate appropriate technical and organisational

measures while designing processing systems, ensuring data security through technology after considering all processing factors. Such protective measures may involve sensitive data encryption, pseudonymisation, and data minimisation to ensure security appropriate to the risk. Based on Recital 83 of the GDPR, encryption is the best way to safeguard data during transfer and one way to secure stored personal data, which can act as mitigating risks and can be a factor in mitigating potential fines. Security measures must be tested, assessed and evaluated regularly to ensure effectiveness (Article 32(1)(d) of the GDPR). Furthermore, implementing Data Protection by Design necessitates the appointment of a Data Protection Officer (DPO) and conducting a comprehensive data protection impact assessment (DPIA).

Data Protection Impact Assessment (DPIA)

The PDPA should incorporate a data protection impact assessment (DPIA) similar to Article 35 of the GDPR to meet obligations under the PDPA before developing and implementing policies and practices necessary to ensure full compliance. DPIA is necessary when the processing is likely to result in a high risk to the rights and freedoms of data subjects. DPIA is an evaluation to ascertain the emerging risks in processing data and mitigate the risks. DPIA should be executed from the earliest to put appropriate safeguards to protect personal data, i.e., before deciding what policies and practices they want to implement (Singapore Guide to Data Protection Impact Assessments, 2021). DPIA should focus on the systematic description of the processing operations, processing purposes, the processing operation's necessity and proportionality, and measures envisaged to address the risks. Before conducting a DPIA, they must consult the Data Protection Officers first. The China PIPL also introduced a mandatory Personal Information Protection Impact Assessment (PIPIA), equivalent to DPIA. PIPIA must be conducted before processing sensitive personal information, handling disclosures and transfers of personal data, or processing that impacts an individual's rights or interests (Article 55 of the PIPL). The PIPIA must specify the purpose and methods of processing, the impact of processing on individuals' rights and interests, the level of risk involved and the protective measures taken. PIA reports and processing records must be retained for at least three years. (Article 56 of the PIPL).

Malaysia can adopt this practice into the PDPA 2010. While awaiting the PDPA 2010 amendment, to ensure a smooth transition of this practice, Malaysia PDPD can encourage data users to adopt DPIA as part of taking practical steps to protect personal data by issuing a guide on DPIA similar to Singapore. In 2021, the Singapore Personal Data Protection Commission (PDPC) issued a *'Guide to Data Protection Impact Assessments'* to encourage organisations to adopt DPIA as part of an organisation's 'Data Protection Management Programme' and demonstrate accountability (Guide to Data Protection Impact Assessments, 2021). Data users can use the Guide and consider the most appropriate steps for conducting DPIA. Even though conducting a DPIA is not an obligation under the PDPA, failure to conduct a DPIA does not constitute a breach under the PDPA 2010, and it still can be considered a failure to take practical steps to protect personal data. Suggested provisions on data protection impact assessment under the PDPA 2010, which was inspired by Article 35 of the GDPR, are as follows: -

Requirement for Data Protection Impact Assessment

(1) Data users and data processors shall conduct data protection impact assessments as a part of taking practical steps to protect data before processing data involving new technologies, which is likely to result in a high risk.
(2) The data users and data processors must, in respect of the assessment in subsection (1):-
    (a) seek advice from Data Protection Officer prior to conducting the assessment.
    (b) identify any risk of the proposed collection, use or disclosure of the personal data for the purpose concerned is likely to have on the individual;
    (c) need to be monitored by the data protection officer.
(3) Identify and implement reasonable measures to —
    (a) eliminate the risk;
    (b) reduce the likelihood that the risk will occur; or
    (c) mitigate the risk; and
    (d) comply with any other prescribed requirements.
(4) The result of the assessment: -

(a) should be recorded and maintained, and
(b) may publish their impact assessment results after redacting several sensitive or trade secret information.

(5) The Commissioner may issue a data protection impact assessment guideline.

Data Protection Officer (DPO)

Malaysia PDPA 2010 must make a mandatory appointment of a Data Protection Officer (D.P.O.) who has professional qualities and is an expert in data protection law and practice as stated under Article 37 of the GDPR and Section 11(3) of the PDPA 2012. These best practices have similarities in DPO responsibilities, which include ensuring compliance with personal data regulation, fostering a culture of data protection among employees and letting stakeholders know about personal data protection regulations, handling queries and complaints related to data, alerting management about the potential risk from the practice, and liaising with the authorities on data protection matters. D.P.O. can be either an employee or an external consultant. The DPO should make their official contact details available to the affected data subjects and the authority. The DPO will advise the data users to develop a strategy to face the worst-case scenario, i.e., data breaches or leaks and respond appropriately, including cooperating with the authority to avoid hefty fines and penalties.

The GDPR and Singapore PDPA may have similarities in the requirements for a DPO, but Singapore has made it more focused and specific. Under the GDPR, DPO must have professional qualities, such as expert knowledge of data protection laws and practices. The PDPC's Advisory Guidelines state that DPOs must be trained and certified, have sufficient skills and be knowledgeable. The PDPC has designed the DPO Training Roadmap to assist the DPOs in identifying necessary courses to advance their proficiency. The PDP commissioner is considering including the requirement for appointing a DPO and issuing a guideline on the mechanism of having a DPO. Following Singapore's approach to designing a DPO certification roadmap can be helpful to ensure they understand the legal and practical aspects of dealing with personal data. Similar certifications can standardise the level of DPO proficiency in Southeast Asia.

The China PIPL also imposed a mandatory appointment of a DPO to supervise the processing of personal information and the adopted protection measures if the amount of personal data has reached a specific limit specified by the State cyberspace administration (the limit has not been specified yet). In the event of a violation of the PIPL, the DPO will also be liable and face severe fines and penalties (Article 66 of the PIPL).

The requirement on DPO appointment is one of the proposed amendments to the PDPA that will be tabled in Parliament in 2023 (Lin & Shairi, 2023). Data users should have a DPO responsible for overseeing data processing matters and day-to-day business operations compliance with the data protection regulations. The responsibility of a DPO includes educating employees to ensure the importance of protecting data and to prepare themselves better to respond to data breaches effectively and in timely manner. Suggested provisions on the role and responsibilities of data protection officer under the PDPA 2010, adopted from Article 37 of the GDPR, are as follows: -

Appointment of Data Protection Officer

(1) A data user or data processor shall designate at least a data protection officer in any case where:
    (a) The core activities of processing consist of large-scale personal data; or
    (b) The core activities of processing consist of sensitive data.
(2) The data protection officer may act to represent the data user or data processor.
(3) The data protection officer may be a staff member or delegate to another individual the responsibility conferred by that designation.
(4) The data user or data processor shall publish the contact information of the data protection officer to the data subject and communicate them to the Commissioner.
(5) The designation of data protection officer does not relieve the data user or data processor of any of its obligations under this Act.

Data Breach Notification

Data users can demonstrate accountability by responding effectively and promptly during the incident. How incidents are handled is essential in mitigating the consequences. The measures taken to rectify the situation should be commensurate with the importance of the compromised data and the risks involved. The most critical response during data breaches is to report or notify the authorities and affected individuals. Singapore, the EU and China have imposed mandatory data breach notifications to the authorities and affected individuals. Despite similarities in this data breach response, each jurisdiction has different requirements regarding pre-requisite data breach response, time response, and to whom they should notify.

A timely response is crucial in mitigating the impact of data breaches. The China PIPL imposed mandatory notification to the relevant authorities and affected individuals immediately. The PI handler can choose not to notify affected individuals if they have taken measures to avoid harm caused by the breach (Article 57 of the PIPL). On the other hand, the EU GDPR and the Singapore PDPA have prescribed time specific regarding the notification. When the data controller is aware of the data breach, the GDPR requires the data controller to notify the Supervisory Authority within 72 hours. The data controller must justify the delay if the notification is given after 72 hours (Article 33 of the GDPR). The data controller must notify the affected individual unless they have implemented several measures (Article 34 of the GDPR). Singapore introduced a mandatory data breach notification requirement under the PDPA 2012, effective 1 February 2021. The organisation must notify data breaches to the PDP Commission within three days (26D of the Singapore PDPA 2012). However, before notification is given, organisations need to contain the breach and assess within 30 days whether the data breach is notifiable under the PDPA, i.e. when the breach significantly harms affected individuals or on a significant scale (26D of the Singapore PDPA 2012) (Guide on Managing and Notifying Data Breaches Under the PDPA, 2021). The organisations are strongly encouraged to notify and seek advice from the PDP Commission before informing the affected individual of the breach (Section 26D(2) of the Singapore PDPA 2012).

In addition, to facilitate organisations in identifying, preparing for, and managing data breaches, Singapore PDPC issued a Guide on Managing and Notifying Data Breaches in 2021. The Guide provides a cyber incident response checklist to help organisations develop their incident response plans. The significance of this plan is that organisations can respond to data breaches systematically and promptly. The Guide recommends responsive measures for organisations to handle data breaches with CARE (the acronym for contain, assess, report and evaluate). The organisations need to contain the data breach from further compromise, implement mitigation actions to mitigate the loss and minimise potential harm, assess the root causes and evaluate their incident responses.

In order to better prepare themselves to respond to data breaches quickly and effectively, organisations may also think about creating contingency plans for potential scenarios involving breaches and the actions to be done. The data management strategy must be supported by key personnel. The employees, the DPO and the data breach management team must understand their roles and responsibilities and have a documented chain of command to ensure the organisation's response to data breaches is not delayed unnecessarily. In addition, to facilitate handling data breaches and their recovery, organisations may also consider developing crisis management, communications, and business continuity plans (Guide on Managing and Notifying Data Breaches Under the PDPA, 2021).

The PDPA 2010 does not require data users to notify the Commissioner and affected individuals in case of a breach that may result in significant harm to them. However, data users can voluntarily notify the Commissioner. The PDP Commissioner seriously considers notification data breach requirements to notify the Commissioner within 72 hours of becoming aware of the incident (Public Consultation Paper No. 01 / 2020, 2020). However, the consultation paper has yet to be gazetted as law.

The significance of notification to the PDP is that the Commissioner can start the investigation. After completing the investigation, the Commissioner must issue an enforcement notice to state his opinion based on section 108 of the PDPA 2010. Section 93(2) of the PDPA 2010 provided that any aggrieved party can challenge the decision by appealing at the Appeal Tribunal, and the Tribunal's decision is final. In addition to notifying the Commissioner, the PDPA should require mandatory notifications to the

affected individuals. Notifying affected individuals is essential as it empowers them to take necessary measures to minimise potential losses. For instance, they can change their passwords to prevent further unauthorised access. It is crucial that affected individuals are aware of the breach and can take appropriate actions instead of remaining uninformed. Data users should assess their incident responses and identify necessary steps to prevent similar incidents from happening in the future.

It is better to publish all data breach cases and enforcement decisions on the PDP's website, similar to Singapore's (PDPC websites) and China's (Article 67 of the PIPL). By doing so, the Commissioner's decisions will offer valuable insights and lessons for data users in Malaysia. The publication will encourage the implementation of appropriate measures to prevent similar incidents from happening in the future. It also serves as a reminder to all data users about their respective rights and obligations under the PDPA. Transparency through publication will establish the credibility and efficiency of the data protection authority. Suggested provisions on data breach notification under the PDPA 2010, adopted from Part 6A of the Singapore PDPA 2012, are as follows: -

Notification of Data Breaches

a. Duty to manage a data breach

1. (1) A data user must have in place a data breach handling and response plan in the event of loss, misuse, modification, unauthorised or accidental access or disclosure, alteration or destruction of personal data.

(2) The plan by a data user under subsection (1) must, at a minimum, include: -

(a) escalation procedures and a clear line of responsibility to contain affected data and take remedial actions;

(b) A reasonable and expeditious assessment of whether the data breach is notifiable;

(c) Notification of notifiable data breach to the Commissioner and affected individuals; and,

(d) evaluation of the data breach response.

b. Mandatory Data Breach Notification

2. (1) In the case of a personal data breach, the data user or data processor shall, as soon as practicable, not later than 72 hours after having become aware of it, notify the notifiable data breach to the Commissioner and affected individuals. Where the notification to the Commissioner is not made within 72 hours, it shall be accompanied by reasons to the Commissioner for the delay.

(2) The notification referred to in subsection (1) shall at least:

(a) describe the nature of the personal data breach: -

i. categories of data;

ii. approximate number of data subjects concerned; and,

iii. approximate number of personal data records concerned.

(b) communicate the contact information of the data protection officer

(c) describe the likely consequences of the personal data breach.

(d) describe the measures taken or proposed to be taken by the data user to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

(3) The data user needs to record the data breach details, the implications and remedial action taken.

(4) The Commissioner shall investigate and verify the compliance after receiving the notification.

Notifiable data breaches

1. A data breach is a notifiable data breach if the data breach —
   (a) results in, or is likely to result in, significant harm to an affected individual; or
   (b) is, or is likely to be, of a significant scale.
   (c) in other prescribed circumstances by the Commissioner.

Analysis of the comparison between Malaysia, the EU and Singapore

Malaysia's PDPA 2010 has a narrow scope of application with wide exemptions (sections 2 and 3 of the PDPA 2010). It only applies to processing personal data in commercial transactions within the country. Singapore's PDPA 2012 extends its coverage to organisations processing personal data in Singapore (Section 4 of the PDPA 2012). In contrast, the EU GDPR and China PIPL have extraterritorial applications (Article 3 of the GDPR and Article 3 of the China PIPL). Despite this similarity, the EU GDPR focuses more on where the business is established, while the PIPL focuses more on where the personal information processing activity happens (Thomas Zhang, 2022).

Regarding the Data Protection Impact Assessment (DPIA), Malaysia's PDPA 2010 does not explicitly mention DPIA. However, Singapore's PDPA 2012 encourages DPIA through a 'Guide to Data Protection Impact Assessments' issued by the PDPC. In contrast, the EU GDPR mandates DPIA when the processing is likely to result in a high risk to the rights and freedoms of data subjects, especially in a systematic and extensive evaluation of data subjects using automated processing, including profiling, processing special data on a large scale, or systematic monitoring of a publicly accessible area on a large scale. (Article 35 of the GDPR). The China PIPL also introduced a mandatory Personal Information Protection Impact Assessment (PIPIA), equivalent to DPIA. PIPIA should be conducted before processing sensitive personal information, handling disclosures and transfers of personal data, or processing that impacts an individual's rights or interests (Article 55 of the PIPL).

Concerning the appointment of a Data Protection Officer (D.P.O.), even though the Malaysian PDPA 2010 is silent on the obligation for data users to appoint a D.P.O., several provisions require data users to ascertain and provide contact details of a contact person to the data subjects. The contact person will deal with requests to access and correct personal data or if the data subjects have any inquiries or complaints regarding their data (Section 7(1)(d) of the PDPA 2010 and Regulation 4 of the Personal Data Protection Regulations 2013). This requirement can be interpreted as almost similar to having a DPO, but rather as a contact person. The role and responsibilities of the contact person are much narrower than those of a D.P.O. The Singapore PDPA 2012 and the EU GDPR mandate the appointment of a D.P.O. (Section 11(3) of the PDPA 2012 and Article 37 of the GDPR). China's PIPL also requires the appointment of a DPO for organisations processing a certain amount of personal information. However, the specific threshold is yet to be specified (Article 52 of the PIPL).

Regarding data breach notification requirements, Malaysia's PDPA 2010 does not require mandatory notification to the PDP Commissioner, but it can be done voluntarily. The Singapore PDPA and the EU GDPR have prescribed time specific regarding the notification. Singapore's PDPA 2012 mandates data breach notification to the PDPC for notifiable breaches within three days after the day the organisation makes that assessment (Part 6A of the PDPA 2012) (Amendment 2020). Similarly, The GDPR imposed the data controller to notify the Supervisory Authority within 72 hours. The data controller must justify the delay if the notification is given after 72 hours (Article 33 of the GDPR). China's PIPL mandates a data breach notification to the relevant authorities and affected individuals immediately. The PI handler can choose not to notify affected individuals if they have taken measures to avoid harm caused by the breach (Article 57 of the PIPL)

Law / subject matter	Malaysia PDPA 2010	Singapore PDPA 2012	EU GDPR	China PIPL
Scope of the application	Applicable to a person who processes the data or controls the personal data process for commercial transactions in Malaysia (Section 2).	Applicable to organisations processing personal data in Singapore (Section 4).	Applicable to entities holding and processing EU residents' data regardless of geographic location (Article 3).	Applicable to any organisation processing the personal information of Chinese citizens in China and outside China (Article 3).
Data Protection Impact Assessment (DPIA)	DPIA is not mentioned under the Act.	DPIA is encouraged through a guide on Data Protection Impact Assessments issued by the PDPC.	DPIA is mandatory when the processing is likely to result in a high risk to the rights and freedoms of natural persons . (Article 35)	DPIA is mandatory (before processing sensitive personal information, disclosures and transfers of personal information, or processing personal information will impact individuals' rights and interests)(Article 55).
Appointment of Data Protection Officer (D.P.O.)	The appointment of a D.P.O. is not mentioned under the Act.	The appointment of a D.P.O. is mandatory (Section 11(3)).	The appointment of a D.P.O. is mandatory (Article 37).	The appointment of a D.P.O. is mandatory when the PI handler processes a certain amount of personal information(Article 52).
Data breach notification	Data breach notification can be done voluntarily.	Data breach notification to the PDPC is mandatory for notifiable data breaches within 3 days (Part 6A) (Amendment 2020).	Data breach notification to the supervisory authority is mandatory within 72 hours (Article 33).	Data breach notification to the relevant authorities is mandatory (Article 57).
Fines and penalties	Failure to comply with 7 data principles is punishable by a fine of up to RM 300,000 or imprisonment for up to two years or both. (Section 5(2)) Unlawful collection of personal data is punishable by a fine is up to RM 500,000 or imprisonment for up to three years or both (Section 130(7)).	Percentage revenue-based fines. Organisations can be fined 10% of their annual turnover in Singapore exceeds SGD 10 million or SGD 1 million, whichever is higher (section 48J).	Percentage revenue-based fines. The fines and penalties for lesser offences are €10 million or 2% of annual global turnover. The maximum is €20 million or 4% of annual worldwide turnover, whichever is higher (Article 83).	In minor violation, they will be liable for a fine of up to RMB 1 million, and the responsible person in charge will be liable for up to RMB 100,000. In a severe violation the PI handler will be liable to a fine of up to RMB 50 million or 5% of the annual turnover, and the responsible person in charge will be liable for a fine of up to RMB 1 million and prohibited from holding senior management positions and roles for a certain period (Article 66).

Table 1. Analysis of the Comparison between Malaysia, the EU and Singapore

The table above compares data protection practices under four different jurisdiction regulations: Malaysia's PDPA 2010, Singapore's PDPA 2012, the European Union's GDPR, and China's PIPL. Each law is evaluated based on several key aspects: scope of application, Data Protection Impact Assessment (DPIA), the appointment of a Data Protection Officer (D.P.O.), data breach notification requirements, and fines and penalties for non-compliance.

Lastly, concerning fines and penalties for non-compliance, Malaysia's PDPA 2010 imposes fines and imprisonment for failure to comply with data principles, a fine of up to RM 300,000 or imprisonment for up to two years or both (Section 5(2) of the PDPA 2010 and unlawful collection of personal data is punishable by a fine is up to RM 500,000 or imprisonment for up to three years or both (Section 130(7) of the PDPA 2010. Singapore's PDPA 2012 allows fines of up to 10% of an organisation's annual turnover or SGD 1 million, whichever is higher (section 48J of the PDPA 2012). The EU GDPR imposes Percentage revenue-based fines, with lesser offences attracting fines of up to €10 million or 2%, and more severe violations up to €20 million or 4% (Article 83 of the GDPR). China's PIPL imposes fines for minor violations, with authorities having the discretion to impose corrective measures or confiscate illegal gains. For severe violations, fines can go up to RMB 50 million or 5% of annual turnover, and responsible persons may face additional penalties. The PIPL imposed fines on individuals who are responsible for PI protection. The responsible person in charge will be liable for a fine of up to RMB 1 million and prohibited from holding senior management positions and roles for a certain period (Article 66).

Conclusion

It is necessary to have a data security framework that consists of preventive, detective, and responsive measures to protect valuable data. Data users need a strategic plan to prevent and manage data breaches appropriately. The EU GDPR, the Singapore PDPA 2012 and the China PIPL have similarities in protecting personal data. These regulations imposed a mandatory appointment of data protection officers, mandatory data breach notification to the authority and data protection impact assessments as part of their data security framework. Despite their similarities, each regulation has different requirements in practice. Malaysian policymakers may selectively adopt best practices in data security frameworks from other jurisdictions to strengthen data security measures in protecting data and managing data breaches. The Malaysian PDPA 2010 did not specify incident responses, but certain obligations on handling breach incidents are scattered under several relevant regulations. Policymakers may consider adopting other jurisdictions' practices in preparation for a data breach exit strategy. The PDPD should provide appropriate guidance on handling data breaches, similar to the Singapore PDPC's Guide. Data breach management plans should be done early to ensure data users manage and respond to data breaches more effectively. Data users can use the Guide to create and execute practical management plans at the early stages of data processing, ensuring a prompt and systematic response. The PDPD can also make specific recommendations but not exhaustively address every scenario nor specify the processes or systems because every data breach has different circumstances and associated risks, and the response needs to be tailored to the particular context. Data users can conduct periodic breach exercise drills to assess their management plans' adequacy and efficiency. These drills will help the key personnel involved in data breach management become familiar with their roles and understand the necessary actions to be taken. No industry is immune from data breaches ("2023 Data Breach Investigations Report | Verizon," 2023). It will be more efficient if the application of the PDPA is not only specific to commercial transactions but also applicable to personal data in non-commercial transactions and government agencies (Sections 2 and 3 of the PDPA 2010). The efficient measures and response will maintain the users' confidence and attract more investors while at the same time giving data users a competitive advantage operating in international trade.

References

2023 Data Breach Investigations Report (DBIR). (2023). In *Verizon Enterprise Solutions*. Retrieved March 26, 2024, from https://www.verizon.com/business/resources/reports/2023-data-breach-investigations-report-dbir.pdf

Agrawal, D., Bernstein, P. A., Bertino, E., Davidson, S. B., Dayal, U., Franklin, M., Gehrke, J., Haas, L. M., Halevy, A., Han, J., Jagadish, H. V., Labrinidis, A., Madden, S., Papakonstantinou, Y., Patel, J. M., Ramakrishnan, R., Ross, K. A., Shahabi, C., Suciu, D., . . . Widom, J. (2011). *Challenges and opportunities with Big Data 2011-1*. Purdue University. https://docs.lib.purdue.edu/cctech/1/

Ali Alibeigi, & Abu Bakar Munir. (2020). Malaysian personal data protection act, a mysterious application. *University of Bologna Law Review*, *5*(2), 362-374.

Beebeejaun, A. (2019). Privacy laws in the context of Fintech Industry in Mauritius: A comparative study. *International Journal of Law, Humanities & Social Science, 3*(3), 23–37.

Chandrasekaran, D. P., Zulkifli, I. H. B. M., Anis, A. M., & Han, Y. S. (2023, February 17). *Personal Data Protection Act 2010 under the New Government: Updates to the proposed amendments in 2023*. Lexology. https://www.lexology.com/library/detail.aspx?g=a6ddd77f-eb48-463e-aaec-ab9174520113

Encryption - General Data Protection Regulation (GDPR). (n.d.). General Data Protection Regulation (GDPR). Retrieved March 26, 2024, from https://gdpr-info.eu/issues/encryption/

Fam, C. (2022, August 29). Data breaches rising rapidly. *The Star*. https://www.thestar.com.my/tech/tech-news/2022/08/29/data-breaches-rising-rapidly

Gaidarski, I., & Kutinchev, P. (2019). Using big data for data leak prevention. *IEEE*.

ICO. (n.d.). *UK GDPR data breach reporting (DPA 2018)*. Information Commissioner's Office. Retrieved March 26, 2024, from https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/

General Data Protection Regulation (the Regulation (EU) 2016/679)

Jochen M. Schmittmann, & Chua Han Teng. (2020, January 23). *Malaysia: Selected issues*. IMF. Retrieved March 26, 2024, from https://www.imf.org/en/Publications/CR/Issues/2020/02/27/Malaysia-Selected-Issues-49106

Kaur, D. (2022, August 16). *iPay88 breach: Is Malaysia losing the data privacy protection game?* Tech Wire Asia. Retrieved March 26, 2024, from https://techwireasia.com/2022/08/ipay88-breach-is-malaysia-losing-the-data-privacy-protection-game/

Loheswar, R. (2022, December 31). Major data breaches in Malaysia in the past 24 months. *Malay Mail*. Retrieved March 26, 2024, from https://www.malaymail.com/news/malaysia/2022/12/31/major-data-breaches-in-malaysia-in-the-past-24-months/47722

Md Toriqul Islam., Abu Bakar Munir., & Mohammad Ershadul Karim. (2021). Revisiting the right to privacy in the digital age: A quest to strengthen the Malaysian data protection regime. *Journal of Malaysian and Comparative Law (JMCL), 48*(1), 49-80.

NIST. (n.d.). *Data security*. Retrieved March 26, 2024, from https://www.nccoe.nist.gov/data-security

Olejarz, J. (2015, July 27). *Why cybersecurity is so difficult to get right*. Harvard Business Review. Retrieved March 26, 2024, from https://hbr.org/2015/07/why-cybersecurity-is-so-difficult-to-get-right

Personal Data Protection Act 2010 (Act 709)

Personal Data Protection Act 2012 (2020 Ed.) (Singapore)

Personal Data Protection Commission Singapore. (2021, September 14). *Guide to data protection impact assessments*. PDPC. Retrieved March 26, 2024, from https://www.pdpc.gov.sg/help-and-resources/2017/11/guide-to-data-protection-impact-assessments

Personal Data Protection Commission Singapore. (n.d.). *Guide on managing and notifying data breaches under the PDPA*. PDPC. Retrieved March 26, 2024, from https://www.pdpc.gov.sg/help-and-resources/2021/01/data-breach-management-guide

Personal Data Protection Regulations 2013 (P.U. (A) 335)

Personal Information Protection Law (China)

PricewaterhouseCoopers. (2022). *PwC's global economic crime and fraud survey 2022*. PwC. Retrieved March 26, 2024, from https://www.pwc.com/gx/en/services/forensics/economic-crime-survey.html

PricewaterhouseCoopers. (n.d.). *PwC's global economic crime survey 2016 (Malaysia report)*. PwC. Retrieved March 26, 2024, from https://www.pwc.com/my/en/publications/gecs-2016-my-report.html#:~:text=Economic%20crime%20from%20the%20board,fraud%20among%20businesses%20in%20Malaysia

Public Consultation Paper No. 01 / 2020. (2020).

Solove, D. J., & Citron, D. K. (2017). Risk and anxiety: A theory of data breach harms. *Texas Law Review*, *96*, 737. https://scholarship.law.bu.edu/faculty_scholarship/616

Sonny Zulhuda. (2010). *Information security in Malaysia: A legal framework for the protection of information assets* [PhD dissertation, International Islamic University Malaysia (IIUM)].

Supramani, S. (2023, February 5). Why are data breaches and leaks still happening? *The Star*. Retrieved March 26, 2024, from https://www.thestar.com.my/news/focus/2023/02/05/why-are-data-breaches-and-leaks-still-happening

The Economist. (2017, May 6). The world's most valuable resource is no longer oil, but data. *The Economist*. Retrieved March 26, 2024, from https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data

The Office of Chief Statistician Malaysia, Department of Statistics Malaysia. (2022, July 29). *Current population estimates, Malaysia, 2022*. Ministry of Economy Department of Statistic Malaysia. Retrieved March 26, 2024, from https://www.dosm.gov.my/portal-main/release-content/current-population-estimates-malaysia-2022

Thomas Zhang. (2022, May 18). PIPL vs GDPR - Key differences and implications for compliance in China. China Briefing. https://www.china-briefing.com/news/pipl-vs-gdpr-key-differences-and-implications-for-compliance-in-china/