# Recent Reforms to the Personal Data Protection Act 2010 and Its Implications for Business Organisations in Malaysia

**Zaiton Hamin[1]*, Saslina Kamaruddin[2], Hafatin Natrah Md Noh[3], Mohd Bahrin Othman [4] & Ani Munirah Mohamad [5]**

**[1&4]Faculty of Law, Universiti Teknologi MARA (UiTM) Shah Alam, Selangor, Malaysia**

**[2]Faculty of Management and Economics, Sultan Idris Education University, Tg Malim, Perak, Malaysia**

**[3]Faculty of Accountancy, Management & Economics, New Era University College, Kajang, Malaysia**

**[5]School of Law and Centre for Testing, Measurement and Appraisal (CeTMA), Universiti Utara Malaysia Kedah, Malaysia**

**DOI: https://dx.doi.org/10.47772/IJRISS.2025.90400033**

**Received: 14 March 2025; Accepted: 18 March 2025; Published: 26 April 2025**

## ABSTRACT

The advancement of the Internet and social media platforms has revolutionised human communication and interactions in the knowledge economy. However, this progress has also introduced significant risks, including cyber scams, misuse of personal data, identity theft, and online harm targeting vulnerable populations such as children. Recent incidents highlight the urgent need for effective data protection legislation. Malaysia's Personal Data Protection (PDP) Act, enacted in 2010 and implemented in 2013, is designed to address these concerns. However, the security of personal data remains a critical issue, evidenced by the rising number of data breaches. This paper focuses on the newly amended PDPA of 2024, assessing its provisions against the data protection framework in the United Kingdom and analysing its ramifications for businesses operating in Malaysia. The qualitative research methodology, which includes doctrinal and comparative legal analysis of primary sources, reveals that protecting personal data is an ongoing and formidable challenge. Key issues such as data sharing, the right to erase personal data, and the role of the Data Commissioner remain inadequately defined in Malaysia's legal framework. Businesses must promptly review and update their policies and procedures to comply with the new legal requirements.

**Keywords**: Data Protection, Data Breach Notification, Data Controller, Data Portability Right, Trans-border Data Transfer.

## INTRODUCTION

The digital era presents significant economic opportunities, with the Malaysian government facing the pressing need to mitigate the risks associated with digital platforms. Safeguarding personal data is not merely a regulatory requirement; preserving Malaysians' data privacy is paramount. In 2024, the digital economy accounted for 23 per cent of the gross domestic product, and projections indicate this figure will rise to 25.5 per cent by 2025, alongside substantial investments.

Despite the Personal Data Protection (PDP) Act 2010 coming into force in 2013, personal data security remains an undeniable concern, underscored by alarming data breach statistics. The Personal Data Protection Commissioner's office reported a staggering 41 per cent increase in data breach notifications in the first quarter of 2024, with complaints rising sharply from 157 in 2023 to 288 in just the first half of 2024. This trend must prompt immediate action as data breaches expose individuals to increased risks of exploitation.

The 2024 amendment to the PDPA is a necessary response to the rising threats and enhances provisions related to personal data processing by international standards. Several overdue changes elevate the legislation's comprehensiveness, addressing critical gaps identified in earlier versions.

This paper introduces pressing data protection issues and provides a historical overview of the 2024 Amendment Act. Next, the study dissects significant changes enacted by the 2024 Act in comparison with the UK legal framework, ultimately exploring the implications of these changes for business organisations in Malaysia.

## Legislative History Of Pdp (Amendment) Act 2024

In 2020, the Personal Data Protection Department released a public consultation paper to review the outdated Personal Data Protection Act (PDPA) 2010. This review identified 22 proposed improvements to the Act. In 2022, the Minister of Communication and Multimedia announced plans to present certain amendments to the PDPA 2010 in Parliament by October 2022. These proposed changes include the appointment of a data protection officer, mandatory notification of data breaches, compliance with security principles for data processors, implementation of data portability rights and restrictions on data transfers to certain blocked countries.

However, the progress of these proposals was interrupted by the dissolution of the Malaysian Parliament on October 10, 2022, followed by a general election and a change in government to the Anwar Ibrahim administration. This political transition delayed the amendment process, as the new government needed time to review and re-evaluate the proposed changes to the PDPA 2010.

On July 10, 2024, the proposed amendment to the Personal Data Protection (PDP) Act 2010 was presented for its first reading in Dewan Rakyat. The bill, introduced by Digital Minister Gobind Singh Deo, had undergone its second reading during the same legislative session. It received royal assent on October 9, 2024, and was published in the Gazette on October 17, 2024. The 2024 Amendment Act, which contained similar proposed changes to those of the 2022 one, aims to enhance the provisions governing the processing of personal data to align with international standards and best practices.

## Crucial Reforms To Pdpa 2010

### Replacing the Term "Data Users" with "Data Controllers"

The nomenclature change occurs in Section 2 of the 2024 Act. According to Section 4 of the previous PDPA, a data controller is a person who processes any personal data, either alone or jointly with others, or has control over or authorises the processing of personal data. In contrast, a data processor is any person, excluding employees of the data user, who processes personal data solely on behalf of the data user and does not process it for their purposes (as defined in Section 4 of the PDPA 2010).

Unlike the UK Data Protection Act 2018, the definition of a data controller is broader, encompassing specific bodies and individuals that act on behalf of the Crown and Parliament. This terminology update aims to align with the terms used in other data protection frameworks, mainly the UK and the European Union General Data Protection Regulation (EU GDPR).

### Exclusion of Deceased Individuals from the Scope of PDPA

The PDPA 2010 does not address whether the personal data of deceased individuals is included. However, under section 3(f) of the 2024 Amendment Act, deceased individuals are explicitly excluded from the definition of 'data subject.' As a result, since the PDPA defines personal data about data subjects, processing personal data belonging to deceased persons will no longer be covered by the PDPA.

### Inclusion of Biometric Data as Sensitive Personal Data

The previous Personal Data Protection Act (PDPA) 2010 did not specifically address biometric data. However, Section 4 defines "sensitive personal data" as any personal data related to a data subject's physical or mental health, political opinions, religious beliefs, or other similar beliefs. It also includes data regarding the commission or alleged commission of any offence and any other personal data determined by the Minister through an order.

The 2024 Amendment Act expanded the definition of sensitive personal data to include "biometric data." According to the new section 3(b), "biometric data" refers to any personal data derived from the technical processing of an individual's physical or behavioural characteristics. In today's cyberspace context, examples of biometric data encompass information processed for facial recognition, fingerprint verification, voice recognition, and retinal scans.

In the UK, the concept of biometric data is broader than it is under Malaysian law. According to Article 4(14) of the UK GDPR, biometric data is defined as "personal data resulting from specific technical processing related to the physical, physiological, or behavioural characteristics of a natural person, which allows or confirms the unique identification of that person, such as facial images or fingerprint data." Unlike the Malaysian framework, biometric data in the UK is classified as a special category of sensitive data under Article 9 only when used to uniquely identify an individual (Information Commissioner Office, 2018). This legal position indicates that the purpose of processing biometric data is more important than the nature or type of data itself.

**New Mandatory Data Breach Notification Obligation**

One of the primary changes in the 2024 Amendment Act is the new obligation for data controllers to notify the Commissioner and affected data subjects of personal data breaches. Under the old PDPA 2010, there was no specific requirement for breach notification. This position has now changed, as section 12B (1) states that when a data controller reasonably believes a personal data breach has occurred, they must notify the Commissioner as soon as practicable in a manner and form determined by the Commissioner. However, the new mandatory data breach notification requirement is ambiguous. It mandates that data controllers notify the Commissioner without specifying a time frame, mentioning only "as soon as practicable" upon reasonable belief of a personal data breach. As defined in the new section 3(d), a personal data breach encompasses any breach, loss, misuse, or unauthorised access of personal data.

Additionally, if the breach causes or is likely to cause significant harm to the data subject, the data controller must inform the data subject without unnecessary delay (section 12B (2)). The Act similarly does not specify a time frame for this notification, instead using the vague term "without unnecessary delay." Furthermore, the Act does not define what constitutes 'significant harm.' In a data breach context, the potential harm is significant and multifaceted, affecting organisations and individuals physically, psychologically, and reputatively. Material or physical harm from data breaches often results in identity theft and substantial financial losses (Romanosky et al., 2010). Individuals affected by data leakages may experience significant psychological harm, including emotional distress, anxiety, and a heightened fear of identity theft or fraud, which can lead to long-term mental health issues (Kilovaty & Kilovaty, 2021). Reputational harms that result directly from data breaches may lead to significant trust erosion. Organisations that experience data breaches suffer considerable reputational damage, eroding consumer trust and resulting in potential business losses (Munir et al., 2024).

In contrast to the UK legal framework, the 2024 Amendment Act lacks specific requirements regarding the details of this obligation, such as notification thresholds and timeframes (Pillai et al., 2024). In the UK, data controllers must notify the Information Commissioner immediately or within 72 hours in case of a breach (Information Commissioner's Office, 2018). This notification must explain the reason for any delays and include details about the nature of the data breach, such as the approximate number of affected data subjects and the categories and approximate number of data records involved. Other requirements include providing the name and contact details of a point of contact for additional information, describing the likely consequences of the breach, and outlining the measures taken to address the breach, including any efforts to mitigate its adverse effects (Information Commissioner's Office, 2018).

However, the legal vacuum created by the Amendment Act 2024 is now filled by the Data Breach Notification Guidelines (DBN Guidelines). The Data Protection Department issued and published the DBN Guidelines on February 26, 2025. Under Paragraph 4, business organisations must notify the Commissioner only if the personal data breach causes or is likely to cause 'significant harm'. Under Paragraph 4(3), such harm is where there is a risk that the data is being breached and:

a) It may result in physical harm, financial loss, an adverse effect on credit records, or damage or loss of property.

b) It may be misused for illegal purposes.

c) It consists of sensitive personal data.

d) It consists of personal data and other information, which, when combined, could potentially enable identity fraud.

e) It is of a 'significant scale' (if the number of affected data subjects exceeds 1000). In contrast, in Singapore, under the Personal Data Protection (Notification of Data Breaches) Regulation 2021, the significant scale is only 500 data subjects.

Similar to the UK legal position, the timeframe to notify the Commissioner is as soon as practicable and 72 hours after the breach (Para 4(4)). Failure to comply with these data breach notification requirements can result in a maximum fine of RM250,000 and a maximum jail sentence of two years or both (section 12B (3)). However, the DBN guidelines state that a data controller must explain in writing the reasons for the delay with supporting evidence for failure to notify within 72 hours (Para 4(5)). It is also important to note that the required information for notification may be provided in phases if simultaneous submission is not feasible, offering data controllers some flexibility (Para 4(6).

**New Obligation to Appoint Data Protection Officer**

The old PDPA 2010 was silent on the requirements for data users to appoint data protection officers (Sugiantari, 2024). However, those registered under the PDPA 2010 and the Personal Data Protection (Class of Data Users) Order 2013 must designate a compliance officer. The details of this officer must be included in the registration form (Hui Lynn Tan, 2024). Additionally, the Code of Practice for Private Hospitals in the Healthcare Industry recommends that data users appoint a data protection officer to ensure adherence to the Code and the PDPA (Hui Lynn Tan, 2024).

Section 12A (1) of the 2024 PDPA mandates that data controllers and/or data processors appoint a data protection officer (DPO) for their organisations. The appointed DPOs must be registered with the Commissioner, who will oversee the compliance of the data controller or processor with the PDPA (Section 12A (3)). It is important to note that appointing a DPO does not relieve the data controller or processor of liability (Section 12A (4)). The 2024 Act does not specify penalties for failing to comply with the DPO appointment requirement. Like the provisions for data breach notifications discussed earlier, the 2024 Amendment Act lacks detailed information regarding this requirement. Further specifics, such as the minimum qualifications or expertise necessary for DPOs, are outlined in the DPO Guidelines developed by the Personal Data Protection Commissioner, which will be discussed in the next part of this paper.

However, failure to appoint a DPO in Singapore may lead to a preliminary investigation by the commission. Furthermore, failure to cooperate with the investigation will constitute an offence punishable with a maximum fine of SGD10,000 or a maximum imprisonment term of 12 months or both. A company may be subject to a fine of SGD100,000.

In the UK, the requirement to appoint a Data Protection Officer (DPO) is primarily governed by the General Data Protection Regulation (GDPR). This regulation mandates that specific organisations designate a DPO to ensure compliance with data protection laws. Unlike in Malaysia, where the regulations do not specify which types of organisations need to appoint a DPO, the GDPR requirement is particularly relevant for entities engaged in high-risk processing activities. These include large-scale monitoring of individuals or the processing of sensitive data (Moerel, 2016).

Article 32 of the GDPR outlines the qualifications and responsibilities of the DPO, highlighting the importance of having professional expertise in data protection law (Wiese, 2024). The DPO is responsible for overseeing all matters related to data protection and ensuring that the organisation adheres to the principles of

the GDPR (Wiese, 2024). Additionally, organisations must provide the DPO with sufficient resources and access to personal data to effectively carry out their duties (Wiese, 2024).

**Increased Penalties for Breach of the Personal Data Protection Principles**

Under Section 5(2) of the old Personal Data Protection Act (PDPA) 2010, non-compliance with the seven personal data principles resulted in a punishment of up to RM300,000 and/or a maximum imprisonment of two years. These principles include: 1. General Principle (Section 6) 2. Notice and Choice Principle (Section 7) 3. Disclosure Principle (Sections 8 and 39) 4. Security Principle (Section 9) 5. Retention Principle (Section 10) 6. Data Integrity Principle (Section 11) 7. Access Principle (Section 12). The 2024 Amendment Act increases the maximum penalty for breaches of those Principles to RM1,000,000 and/or three years of imprisonment or both (section 5 (b)(ii)).

The UK's penalties for violating data protection principles are primarily enforced by the Information Commissioner's Office (ICO). These civil penalties can include significant monetary fines and potential criminal sanctions. The severity of these penalties emphasises the importance of protecting personal data under the General Data Protection Regulation (GDPR) and the Data Protection Act. The ICO can impose fines of up to £500,000 for serious breaches of data protection laws (Nettleton & Willison, 2010). Under GDPR, fines can go as high as 4 per cent of a company's global turnover, which can be incredibly substantial for larger organisations.

In contrast to Malaysia's criminal sanctions approach, recommendations have been made for introducing criminal penalties, including imprisonment, for serious misuse of personal data, particularly in the healthcare sector (Hawkes, 2015). The ICO has previously advocated jail sentences of up to two years for severe violations, indicating a movement towards stricter enforcement (Warren, 2007). This push for criminal sanctions also reflects a growing recognition of the need for robust protection against data misuse. This dual approach aims to enhance public trust in data handling practices.

**Extension of the Security Principle to Data Processors**

Before 2024, the PDPA 2010 applied solely to data controllers, imposing no legal obligations on data processors. However, with the introduction of the new section 5 (1A), data processors who process personal data on behalf of data controllers must comply with the Security Principle outlined in section 9 of the PDPA. Non-compliance with the PDPA will result in data processors facing the penalties previously mentioned. According to the Security Principle, data processors must take practical steps to protect personal data from loss, misuse, alteration, destruction, unauthorised access, accidental access, modification, or disclosure. Furthermore, data processors must provide adequate assurances regarding the technical and organisational security measures for their processing and take reasonable steps to ensure adherence.

UK data processors must comply with the security principles set out in the Data Protection Act (DPA) and Article 32 of the General Data Protection Regulation (GDPR). These regulations mandate that data processors implement appropriate technical and organisational measures to ensure the security of personal data (Burton, 2020; Christiana, 2024). Compliance is a legal obligation essential for maintaining trust and protecting individuals' privacy.

The legal framework outlines eight data handling principles, emphasising that data must be processed securely and following individuals' rights (Länder, 2011). Furthermore, Article 32 of the GDPR explicitly requires data processors to adopt security measures that protect personal data from breaches (Burton, 2020). Data processors must implement security measures that are suitable for the risks involved. Such measures include encryption, access controls, and regular security assessments (Christiana, 2024). The GDPR also mandates that processors notify data controllers of data breaches, promoting transparency and accountability (Burton, 2020).

Non-compliance with these security principles can result in significant penalties, including fines and damage to an organisation's reputation (Azam et al., 2024). Organisations may also face legal action from individuals whose data has been compromised due to insufficient security measures (Länder, 2011). While adhering to

these security principles is vital, some argue that the stringent requirements may inhibit innovation and operational flexibility, particularly for smaller businesses that may struggle with compliance's associated costs and complexities.

**New Right to Data Portability**

Data portability is one of the rights of data subjects, including the right to access, the right to rectify personal data, and the right to prevent processing. In the UK, Article 21 of the UK GDPR establishes the right to data portability, allowing individuals to receive personal data provided to a controller in a structured, commonly used, and machine-readable format. It also allows individuals to request that a controller transmit this data directly to another controller. Unlike the EU approach, the UK consumer-centric model aims to empower individuals regarding their data and enhance consumer rights (Wen Long, 2022). However, this approach raises concerns about potentially lowering data protection standards.

In Malaysia, before 2024, data subjects did not have rights to data portability under the PDPA 2010. However, a newly created Section 43A of the Amendment Act 2024 introduces the right to data portability, enabling data subjects to request the direct transmission of their data from one data controller to another. This request must be made electronically to the data controller in writing. It is important to note that this right is not absolute and is subject to the technical feasibility and compatibility of the data format (Section 43A(2)). The data controller must complete the transmission of the personal data upon receiving such a request within the prescribed period. Like the other changes mentioned, the 2024 Act does not specify the scope and application of this right. Further details about implementing this right are expected to be outlined in the upcoming Right to Data Portability Guidelines.

**Removal of Allowlisting Regime for Cross-Border Data Transfers**

The UK's data protection law is primarily governed by the Data Protection Act 2018 (DPA) and the UK GDPR, which serves as the UK's implementation of the EU GDPR. These legislations strengthen the rights of individuals and establish new rules for transferring data outside the European Union. The UK GDPR applies to the processing of personal data of individuals in the UK by organisations that are not based in the UK. This legislation applies when the processing activities involve offering goods or services to these individuals or monitoring their behaviour within the UK (Nóra, 2024; Harcourt, 2023; Kuner, 2023).

The UK's data protection law provides several modalities for cross-border data transfer, such as below:

a. Adequacy and equivalent modality

The EC has provided the UK with adequate decisions, allowing the free flow of personal data between the UK and the EU. These decisions are based on the UK's commitment to maintaining data protection 'essentially equivalent' to EU law (Harcourt, 2023; Kuner, 2023; Murray, 2023).

b. Standard Contractual Clauses (SCCs)

Organisations can use these contractual clauses to transfer personal data outside the EU. The UK adopts SCCs to allow organisations to transfer data to jurisdictions without adequacy decisions (Martin, 2023; Kuner, 2023; Murray, 2023).

c. Binding Corporate Rules (BCRs)

These are internal rules recognised by the UK that organisations can implement to transfer personal data within their companies (Martin, 2023; Celeste, 2021; Kuner, 2023; Murray, 2023).

d. Derogations

This modality allows the transfer of personal data to jurisdictions without adequacy decisions under specific conditions such as explicit consent, contractual necessity, or for the establishment, exercise, or defence of legal

claims (Martin, 2023; Kuner, 2023; Murray, 2023).

In Malaysia, before 2024, Section 129(1) of the Personal Data Protection Act (PDPA) 2010 allowed the Minister to create an allowlist of jurisdictions outside of Malaysia to transfer personal data. The Minister also had the authority to determine the circumstances under which cross-border transfers of personal data were necessary for the public interest. However, this allowlisting mechanism for cross-border data transfers has not been utilised since the PDPA was enacted.

The 2024 Amendment Act reverses previous changes and establishes a general legal framework for transferring personal data to jurisdictions outside Malaysia in the following situations:

1. The jurisdiction has laws like the Personal Data Protection Act (PDPA).

2. The jurisdiction provides adequate protection for processing personal data, equivalent to the protections offered under the PDPA.

The current exemptions for cross-border data transfers under the PDPA 2010 (such as obtaining the data subject's consent or considerations of public interest) are still valid. In line with the previous changes, the forthcoming Cross-Border Data Transfer Guidelines from the Commissioner are expected to clarify the measures that data controllers must take when relying on these conditions for such transfers.

**Implications for Business Organisations**

**Nomenclature Changes**

The impending terminology changes, while primarily cosmetic, will not undermine the fundamental obligations of company data controllers under the PDPA. However, it is imperative that companies promptly update their personal data protection notices, policies, and agreements to align with the new legal framework when the 2024 Act is enforced in three stages this year (Brendan Lai, 2024).

**Biometrics Data**

Companies processing biometric data will face stricter consent requirements as stipulated in section 40, along with enhanced security measures outlined in section 9, which pertain to sensitive personal data under the PDPA (Pillai et al., 2024; Brendan Lai, 2024). For example, in the banking sector, integrating biometric data can significantly enhance the transaction's security (Jayasree & Beatrice, 2024) and operational efficiency and transaction security, particularly when biometrics and AI are integrated to predict user behaviour (Ganguly et al., 2024). Hence, it is essential for companies to meticulously review their documentation, including privacy notices and consent clauses, to ensure compliance with these new mandates.

**Data Breach Notification**

Prior to the publication of the DBN Guidelines mentioned above, in anticipation of the mandatory data breach obligation, business organisations must take immediate action to develop and refine their internal data breach management and reporting procedures (Pilai et al., 2024). However, since February 26 this year, companies must establish a robust data breach notification protocol that follows the DBN Guidelines. They must take proactive and decisive steps to ensure effective communication with the Commissioner and data subjects to fulfil this crucial requirement. Recognising when a data breach occurs is not just a regulatory obligation - protecting individuals' privacy and trust is vital. The primary catalysts of breaches, such as unauthorised access to personal data and the potential harm to data subjects, highlight the urgency of this responsibility (Martin, 2023). Companies can safeguard their stakeholders and enhance their reputation by familiarising themselves with Section 12B and the DBN Guidelines. Taking these steps is a legal necessity, as well as a commitment to ethical business practices and customer confidence.

Furthermore, establishing a robust response plan with a dedicated incident response team is essential for effectively managing data breaches or leaks. This proactive approach allows organisations to investigate

incidents thoroughly, assess their impact, and coordinate timely notifications to those affected (Schwartz & Janger, 2007). Under the DBN Guidelines, companies must immediately assess any data breach. Companies must also promptly contain and mitigate the potential impact upon discovering a breach. They must isolate and disconnect the compromised database or system from the network and suspend or turn off any compromised access rights without delay.

Under Para 4 of the DBN Guidelines, companies must notify the Commissioner within a strict 72-hour timeframe upon detecting a breach. The initial notification must be completed using the designated form provided in the DBN Guidelines or the notification form available on the Personal Data Protection Department website. Companies must include comprehensive details about the breach, including its potential consequences and a precise chronology of the events that led to it (Paragraph 4(4)). Even if a company cannot supply all requested information at the time of notification, it must still provide any available information. Furthermore, any additional information must be submitted incrementally as soon as possible but no later than 30 days from the date of the initial notification (Paragraph 4(6)).

Additionally, to effectively navigate the complexities of the new law, companies must prioritise diligent record-keeping. This duty involves maintaining comprehensive records of any data breaches, including the nature of the affected data and the steps taken in response. Businesses must ensure compliance and build customer trust (Martin, 2023). Under the DBN Guidelines, companies are obligated to maintain data breach records. They must keep records and maintain a register detailing personal data breaches for at least 2 years from the notification date to the Commissioner (Paragraph 4(7)). Companies must document specific information in the register, including a description of the breach, a timeline of events, and the measures taken to contain and recover from the breach.

Paragraph 5 asserts that companies must notify affected data subjects of a data breach if it results in or is likely to result in 'significant harm' to those individuals. This requirement parallels the obligations for notifying the Commissioner. Importantly, unlike the notification to the Commissioner, notification to the data subjects is mandated even if the breach is not of 'significant scale', i.e. less than 1000 data subjects. Companies must notify the affected data subjects without unnecessary delay, which must occur no later than 7 days after informing the Commissioner (Paragraph 5(2)). The notification should be direct and individual, presented in intelligible language suited to the circumstances (Paragraph 5(3)). If direct notification proves impracticable or constitutes a disproportionate effort, companies must employ alternative methods, such as public communication, to effectively inform the affected data subjects (Paragraph 5(4)). The DBN Guidelines, however, do not define what constitutes disproportionate effort.

The information companies are to provide to the affected data subjects is similar to the one in the notification to the Commissioner, including the details of the breach, its potential consequences, the measures taken or proposed to be taken to address the breach, and the measures that data subjects may take to mitigate potential adverse effects (Paragraph 5(2)(a)-(e ) ).

Embracing automated systems for breach notification can significantly enhance compliance efforts. These systems can streamline the analysis of breach information and facilitate prompt, appropriate action (Federgreen & Sachs, 2015) in alignment with the DBN Guidelines. While some may argue about the cost implications, particularly for small and medium-sized enterprises (SMEs), the long-term benefits outweigh the initial investment. Automated systems reduce the risk of human error and free up valuable time for employees to focus on other critical areas of the business. Significantly, automated systems are proactive measures that could safeguard the business from severe penalties, reputational damage, and loss of customer trust that often accompany data breaches.

**Duty to Appoint a DPO**

Before the Commissioner releases the DPO Guidelines on February 26, 2025, companies must proactively recognise and prepare for the newly created obligations to ensure compliance with the forthcoming requirements. They must also identify qualified candidates for the Data Protection Officer (DPO) role and formalise this position. Since February 26, 2025, with the publication of the DPO Guidelines, this duty has become clear and should be prioritised.

Under Paragraph 4(1)-(5), companies must appoint one or more DPOs if their processing of personal data involves personal data exceeding 20,000 data subjects, sensitive personal data, including financial information exceeding 10,000 data subjects or activities that require 'regular and systematic' monitoring of personal data.

Paragraph 4(5)(a)-(e) provides the skills, qualities and expertise that the DPO must possess, including:

a. Knowledge of PDPA and local data protection practices

b. Understand the companies' business and personal data processing operations

c. Understand information technology and data security

d. Personal qualities include integrity, understanding of corporate governance and high professional ethics

e. Ability to promote a data protection culture within the organisation.

Paragraph 4(4) establishes clear qualifications and requirements for a Data Protection Officer (DPO) in Malaysia: the DPO must be a resident, meaning they must be physically present in Malaysia for at least 180 days in a calendar year or be readily contactable by any means. Additionally, proficiency in the national language and English is essential. In contrast, Singapore's DPO does not need to be a citizen or resident. However, the DPO must be readily contactable from Singapore and available during local business hours. If telephone numbers are provided, they must be Singaporean numbers.

However, the DPO Guidelines were silent on the DPO's professional qualifications. Companies can appoint DPOs from their current employees or through outsourcing services on a part-time or full-time basis (Paragraph 4(3)).

Companies must be aware of the responsibilities of the DPO as prescribed by the DPO Guidelines. Under Paragraph 5(1)(a) - (f), these duties include the following:

a. Inform and advise the company on personal data processing

b. Support the company in complying with the PDPA and other related data protection laws and monitor the company's compliance with these laws.

c. Support the company's undertaking of data protection impact assessment

d. Ensure proper data breach and security incident management

e. Act as a facilitator and point of contact for data subjects

f. Act as the liaison officer and the main point of reference for the Commissioner.

Paragraph 6 of the DPO Guidelines explicitly provides the duties of companies once the DPO is appointed, including:

a. Ensuring the DPO is involved in all data protection matters in the company

b. Supporting the DPO in his tasks under para 5(1) above by giving him adequate autonomy

c. Giving the DPO adequate resources to carry out their tasks effectively

d. Allowing the DPO direct access to senior management of the companies.

e. Providing training for the DPO to enable him to do his job efficiently and effectively

f. Companies cannot terminate the DPO who is doing his job under para 5(1)

g. A dedicated business e-mail account must be created for the DPO, which must be separated from the DPO's personal and business e-mail addresses.

h. If the DPO terminates his services or if his services have expired, the company should reappoint the DPO or replace him within a reasonable time. Companies must update the new DPO's information within 14 days of their appointment (Para 8(3)).

Paragraph 8(1)(2) of the DPO Guidelines outlines companies' responsibilities regarding the notification of their Data Protection Officers (DPOs). Companies are required to inform the Commissioner of their appointed DPOs using the online Personal Data Protection System within 21 days from the date of appointment. Additionally, companies must maintain records of their appointed DPOs. According to Paragraph 9, companies must also publish the business contact information of their DPOs on their official websites or through other official media, such as data protection notices or security policies and guidelines. Furthermore, Paragraph 7 authorises the Commissioner to establish mandatory courses, training programs, and benchmarking mechanisms for DPOs in the future.

The obligation to appoint a Data Protection Officer (DPO) may impose administrative burdens and cost implications, often leading to resistance from small and medium-sized enterprises (SMEs). However, the long-term benefits of compliance and risk mitigation decisively outweigh these concerns (Weise, 2024). Appointing a DPO is vital for establishing a culture of accountability and transparency in data handling practices (Emili, 2019). This role ensures compliance and builds trust with stakeholders and data protection authorities (Šidlauskas, 2021). By clearly defining responsibilities and authority (Brendan Lai, 2024), companies must provide relevant training for the DPO. It is essential for organisations to thoroughly review their data protection policies and procedures to define the DPO's role and authority explicitly.

**Increased Penalties for Breach of Data Protection Principles**

Regarding the increased penalties for breaching the Principles, it is crucial to note that, unless proven otherwise (such as when an offence occurs without the data controller's knowledge or if all reasonable precautions and due diligence were observed), company directors, CEOs, COOs, Chief Data Officers (CDOs), Chief Information Officers, and Compliance Officers involved in managing a data controller will be deemed liable for any violations. They can face joint and separate liability alongside the corporate entity for such offences and may incur the specified penalties.

**Data Portability Rights**

The introduction of the right to data portability raises questions about the responsibilities of the stakeholders in the data ecosystem. The unclear responsibilities of data subjects, data controllers and data processors might hinder compliance with the 2024 Amendment Act. Such uncertainty underscores the need for more explicit regulatory guidelines from the Commissioner to ensure all parties understand their obligations. Businesses can thoroughly understand and implement the new data portability rights for data subjects, enhance compliance, improve data management practices, and build greater consumer trust (Janssen et al., 2020). Apart from empowering data subjects, this shift in the right to data portability could lead to a more user-centric approach in data management, where individuals can decide how their data is shared and used (Janssen et al., 2020).

**Transborder Data Transfer**

Regarding transborder data transfer, companies must be aware of the contractual and security measures required to transfer data to jurisdictions without adequate decisions from Malaysia. As best practices, business organisations should conduct transfer risk assessments tailored to their specific risk levels and the maturity of their business (Martin, 2023). To maintain compliance and protect personal data, organisations must stay informed about evolving laws regarding data transfers to other jurisdictions (Martin, 2023). Companies should familiarise themselves with the tools that help ensure compliance with these new provisions, as the importance of due diligence and compliance in international data transfer is increasingly significant. The four modalities previously mentioned in the UK could also apply to similar frameworks in Malaysia if adequacy decisions, Standard Contractual Clauses (SCCs), Binding Corporate Rules (BCRs), and other derogations are in place.

# CONCLUSION

The introduction of the long-awaited Amendment Act in 2024, which has been in development since 2018, represents a significant advancement in Malaysia's data protection regulatory framework. The original purpose of the Personal Data Protection Act (PDPA) was to safeguard individual privacy, build trust in digital transactions, and align with international data protection standards (Cieh, 2013). However, with the rapid advancement of information and communication technology (ICT), Malaysians have increasingly turned to digital platforms for business operations. At the same time, there is a growing demand for robust protections for personal data. Consequently, there is a need to amend the PDPA to update the law, making it more comprehensive and ensuring that it aligns with current international standards and practices for data protection. This alignment is essential for fostering trust in the digital economy and ensuring that Malaysian citizens' data is protected in a manner consistent with global norms. In today's digital landscape, safeguarding sensitive information is not just a responsibility but an imperative for every company.

However, the 2024 Amendment Act does not provide many specifics regarding implementing the new requirements and obligations. These details will likely be included in the guidelines for the Commissioner to develop a range of guidelines to support the changes introduced by the Amendment Act. This suite of guidelines will help clarify the new obligations and enhance data protection practices in Malaysia. These guidelines will include Data Portability Guidelines, Cross-Border Data Transfer Guidelines, Mechanisms, Data Protection Impact Assessment Guidelines, Privacy by Design Guidelines and Profiling and Automated Decision-Making Guidelines.

The 2010 PDPA was primarily established to safeguard personal data in commercial transactions. This emphasis reflects a growing concern regarding handling personal information in business environments, which is crucial in today's data-driven economy. The 2024 Amendment Act will significantly impact how organisations and businesses manage personal data, necessitating changes in data processing practices to ensure compliance with the new legal requirements. Additionally, this recent Act highlights the need for businesses to review and update their policies, procedures, and control measures considering these changes. The 2024 Amendment Act represents progress; however, crucial areas require improvement. These include data-sharing practices, individuals' rights to delete personal data from public digital records, the responsibilities of the Data Commission, and the broader data governance framework, all of which still lack clear definitions. It remains to be seen when the Malaysian government tackles these issues and establishes a more comprehensive data protection law.

Based on the examination of the recent amendments to Malaysia's Personal Data Protection Act (PDPA) 2023 and its implications for business organisations, several policy recommendations can be made:

1. *Strengthen Compliance Mechanisms*: Businesses should be required to implement and document robust data protection policies and practices. Regular audits should be mandated to ensure compliance with the PDPA and any amendments, fostering a culture of accountability.

2. *Data Breach Notification Requirements*: Enhance the clarity and requirements for data breach notifications. Establish mandatory timelines and procedures for notifying affected individuals and the Commissioner about data breaches to improve the timeliness and effectiveness of response measures.

3. *Awareness and Training Programs*: Launch nationwide awareness campaigns to educate businesses and consumers about data privacy rights and responsibilities. Tailored training programs for DPOs and employees who handle personal data can enhance understanding and compliance within organisations.

4. *Data Governance Framework*: Develop a comprehensive data governance framework that clearly defines the roles and responsibilities regarding data protection. This framework should include guidelines on managing trans-border data transfers, data sharing agreements, and handling sensitive personal data.

5. *Enhance the Role of the Data Commissioner*: Empower the Personal Data Protection Commissioner with more substantial enforcement capabilities and resources to effectively oversee compliance, investigate complaints, and act against non-compliance.

6. *Promote International Cooperation*: Encourage collaboration with international data protection bodies and foreign governments to align Malaysia's data protection laws with global standards. This strategy will facilitate smoother trans-border data flows and enhance the country's reputation in international business.

7. *Research and Development*: Foster academic and empirical research on data protection issues to continuously assess the PDPA's effectiveness and its amendments. Regular feedback from industry stakeholders should be integrated to refine this legislation.

8. *Public Consultation on Future Reforms*: Establish a framework for ongoing public consultation with stakeholders, including businesses, consumers, and legal experts, before implementing further changes to data protection laws or before establishing the relevant guidelines stated above.

9. *Focus on Technological Solutions*: Support technological advancements in data protection, such as encryption and secure data storage solutions. Encourage businesses to adopt these technologies as part of their compliance efforts.

10. *Consumer Empowerment Initiatives*: Empower consumers with greater rights to control their personal data, such as improved mechanisms for the above-mentioned data portability rights and the right to request the deletion of their data from various platforms.

By implementing these recommendations, Malaysia can significantly enhance its data protection framework, ensuring better protection for individuals while promoting a trustworthy environment for businesses operating in the digital economy.

## ACKNOWLEDGEMENT

The authors thank the Faculty of Law, Universiti Teknologi MARA (UiTM) Shah Alam, Selangor, Malaysia, for sponsoring this article.

## REFERENCES

1. Ang, W. (2024) Malaysia Introduces Watershed Amendments to Personal Data Protection Act 2010.https://www.dataprotectionreport.com/2024/07/malaysia-introduces-watershed-amendments-to-personal-data-protection-act-2010/.
2. Aw, C. (2024). Malaysia Pushes out Groundbreaking Amendment to Personal Data Protection Act - Impact on Businesses, https://tinyurl.com/mrxybzdf.
3. Azam, N., Michala, A. L., Ansari, S., & Truong, N. B. (2024). Modelling Technique for GDPR-compliance: Toward a Comprehensive Solution. https://doi.org/10.48550/arxiv.2404.13979.
4. Burton, C. (2020). Article 32 Security of processing. Oxford University Press. https://doi.org/10.1093/OSO/9780198826491.003.0068.
5. Cieh, E. L. Y. (2013). Personal Data Protection and Privacy Law in Malaysia (pp. 5–29). Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-33081-0_2.
6. D'Ambrosio, M. (2021). GDPR and its implications for data protection in the UK. Legal Studies Review, 38(2), 200-214.
7. Federgreen, W. R., & Sachs, F. E. (2015). Automated Data Breach Notification. https://patents.google.com/patent/US20150154520A1/en.
8. Ganguly, A. K., Bhattacharya, S., & Chattopadhyay, S. (2024). A Design of Efficient Biometric based Banking System Through AI-Powered Transaction Security Fintech System for Secure Transactions. 6, 492–496. https://doi.org/10.1109/icacite60783.2024.10617391.
9. Harcourt, A. (2023). Data Protection and Privacy Post-Brexit (pp. 181–196). Oxford University Press. https://doi.org/10.1093/oso/9780192899378.003.0010.
10. Hawkes, N. (2015). Tougher penalties, including imprisonment, are urged for misuse of personal data. BMJ, 350. https://doi.org/10.1136/BMJ.H619.
11. Hui, L.T. (2024). Malaysia: Implementation of the Personal Data Protection (Amendment) Act 2024. https://www.dfdl.com/insights/legal-and-tax-updates/malaysia-implementation-of-the-personal-data-

protection-amendment-act-2024/
12. Information Commissioner's Office (2018). Biometric Recognition. https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/biometric-data-guidance-biometric-recognition/biometric-recognition/
13. Janssen, H., Janssen, H., Cobbe, J., Norval, C., & Singh, J. (2020). Decentralised Data Processing: Personal Data Stores and the GDPR. Social Science Research Network. https://doi.org/10.2139/SSRN.3570895.
14. Jayasree, L., & Beatrice, B. A. (2024). Enhancing cybersecurity in banking through implementing biometric systems: a systematic study. ShodhKosh Journal of Visual and Performing Arts, 5(7). https://doi.org/10.29121/shodhkosh.v5.i7.2024.3889.
15. Kilovaty, I. & Kilovaty, M. (2021). Psychological Data Breach Harms, 23 North Carolina Journal of Law &Technology. 1. https://scholarship.law.unc.edu/ncjolt/vol23/iss1/2.
16. Kuner, C. (2023). Protecting EU data outside EU borders under the GDPR. Common Market Law Review, 60(Issue 1), 77–106. https://doi.org/10.54648/cola2023004.
17. Lee, E. (2024) A Comparative Analysis of the Malaysian Personal Data Protection Act 2010 and GDPR. https://tinyurl.com/233vbbnj.
18. Martin, B. R. (2023). International transfers of personal data (pp. 163–197). Edward Elgar Publishing. https://doi.org/10.4337/9781035301874.00022.
19. Moerel, L. (2016). GDPR conundrums - The data protection officer requirement. https://research.tilburguniversity.edu/en/publications/gdpr-conundrums-the-data-protection-officer-requirement.
20. Munir, A. B., & Yasin, S. H. M. (2002). Privacy and Data Protection: A Comparative Analysis with Special Reference to the Malaysian Proposed Law. Sweet & Maxwell, Petaling Jaya.
21. Munir, A. B. & Mohd Yasin, S. H. (2010). Personal Data Protection in Malaysia: Law and Practice. Sweet & Maxwell, Petaling Jaya, Selangor.
22. Nettleton, E., & Willison, C. (2010). Data protection: More powers for the information commissioner. The Journal of Database Marketing & Customer Strategy Management, 17(2), 132–137. https://doi.org/10.1057/DBM.2010.5
23. Pesuruhjaya Perlindungan Data Peribadi (2025). Pekeliling Bil 1 2025, Perlantikan Pegawai Perlindungan Data dan Pemberitahuan Perlanggaran Data
24. https://www.pdp.gov.my/ppdpv1/garis-panduan-dan-pekeliling-perlindungan-data-peribadi-pelantikan-pegawai-perlindungan-data-dpo-dan-pemberitahuan-pelanggaran-data/
25. Romanosky, S., Acquisti, A. & Sharp, R. (2010), Data Breaches and Identity Theft: When is Mandatory Disclosure Optimal? TPRC. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1989594.
26. Sandford, A. (2023). Post-Brexit Guide: What has been the impact — and how did it happen? Euronews. https://tinyurl.com/rhrxbd2h.
27. Sugiantari, A. A. P. W. (2024). Unfolding Data Protection Officer Regulation in Personal Data Protection: Evidence Malaysia. Pakistan Journal of Life and Social Sciences, 23(1). https://doi.org/10.57239/pjlss-2025-23.1.0062.
28. Schwartz, P. M., & Janger, E. J. (2006). Notification of Data Security Breaches. Social Science Research Network. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=908709.
29. Smith, A. (2022). Enforcing data protection laws: Challenges and opportunities. International Legal Journal, 14(2), 75-92.
30. Tobin, D. (2025). What is Data Privacy—and Why Is It Important? https://www.integrate.io/blog/what-is-data-privacy-why-is-it-important.
31. Wenlong, L (2022).Between incrementalism and revolution: How the EU and the UK post-Brexit revamp the GDPR right to data portability. Eleni Kosta and Ronald Leenes (eds), Research Handbook of EU Data Protection Law, Edward Elgar Publishing eBooks.
32. Wiese, S.C. (2024). Position of the data protection officer. Oxford University Press. https://doi.org/10.1093/law/9780192855220.003.0033.
33. Wiese, S.C. (2024). Tasks of the data protection officer. Oxford University Press. https://doi.org/10.1093/law/9780192855220.003.0034.