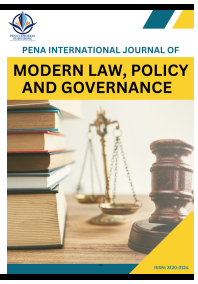
PENA CENDEKIA PUBLISHING
NURTURING IDEAS, ENRICHING KNOWLEDGE

Pena International Journal of Modern Law, Policy and Governance

Journal homepage:
https://penacendekia.com.my/index.php/pijmlpg/index
ISSN: 3120-3124



Safeguarding Trust: The Role of Personal Data Protection Act 2010 and Corporate Standard Operating Procedures in Preventing Consumer's Data Misuse

Intan Marhaenis Sharul Azuan[1], Ajmila Zarif Rusli[1], Farini Aina Khairuddin[1], Farhanin Abdullah Asuhaimi[1,*],Mohd. Lu'ay Khoironi[2]

[1] Department of Law, Fakulti Undang-undang dan Hubungan Antarabangsa, Universiti Sultan Zainal Abidin, 21300 Kuala Nerus, Terengganu, Malaysia
[2] Department of Law, Fakultas Hukum, Universitas Wisnuwardhana, Indonesia

ARTICLE INFO

Article history:
Received 21 August 2025
Received in revised form 16 September 2025
Accepted 10 October 2025
Available online 19 October 2025

Keywords:
Consumer privacy; corporate governance; data breaches; personal data protection

ABSTRACT

Rising cases of personal data misuse in Malaysia have intensified calls for more effective consumer data protection mechanisms. Although the Personal Data Protection Act 2010 (PDPA) establishes the main legal framework for safeguarding personal information, large-scale breaches such as the leakage of 67.5 million personal records between 2011 and 2021, reveal persistent gaps between legal provisions and real-world practices. These incidents not only undermine consumer trust but also expose system weaknesses in both regulatory oversight and corporate compliance cultures. This article examines the issue through a doctrinal legal analysis of the PDPA, supplemented by content analysis of selected corporate compliance measures, with comparative insights drawn from other jurisdictions such as the European Union's General Data Protection Regulation (GDPR) and the Singapore's Personal Data Protection Act 2012. The findings reveal that many data breaches stem less from legislative inadequacies than from weak enforcement of internal standard operating procedures (SOPs), insufficient training within the organizations. The study concludes that effective consumer data protection in Malaysia necessitates a dual approach. On one hand, strict compliance with PDPA obligations must be ensured through active regulatory enforcement, including monitoring, inspections and sanctions. On the other hand, corporations must strengthen internal governance by institutionalising SOPs, investing in continuous staff training, and embedding accountability mechanisms across organizational structures. By fostering stronger synergy between statutory law and corporate self-regulation, companies can safeguard consumer trust, mitigate liability risks, and promote responsible business practices that support long-term sustainability in the digital economy.

* *Corresponding author.*
E-mail address: farhanin@unisza.edu.my

https://doi.org/10.37934/pijmlpg.2.1.115

1. Introduction

Personal data is now one of the most valuable assets in the digital economy, yet it is increasingly vulnerable to misuse. Around the world, data breaches have caused significant economic losses and eroded public confidence in digital systems. In Malaysia, the threat is particularly severe. According to the Malaysian Communications and Multimedia Commission (MCMC), the country reported an average of 15 data breach cases per week in 2023, most of which were linked to ransomware, phishing, and insider negligence [1]. These incidents reveal both the sophistication of modern cyberattacks and the weaknesses of current data protection systems.

A cybersecurity breach can be defined as any unauthorized access or attack on a computer system or network that compromises the confidentiality, integrity, or availability of the information it contains. A data breach occurs when unauthorized parties gain access to personal or sensitive information. These breaches can take multiple forms, including malware infections, phishing campaigns, ransomware attacks, and insider threats, each of which is capable of causing serious financial, reputational, and legal consequences. Often, breaches occur via a three-step process: research, attack, and compromise, where attackers gather intelligence, exploit vulnerabilities, and then infiltrate systems to steal or manipulate data [2]. Recognizing these risks, Malaysia enacted the Personal Data Protection Act 2010 (PDPA) as its principal framework to regulate the collection, processing, and disclosure of personal data. The Act aims to safeguard consumer privacy and establish accountability among data users. It protects individual from any form of abuse in the storage or processing of personal data of individuals, public, and private sectors in Malaysia.

Despite the establishment of the PDPA framework, repeated large-scale data breaches continue to occur in Malaysia, raising serious concerns about the effectiveness of existing safeguards. Over the past two years, the country has witnessed numerous incidents across both public and private sectors. For instance, in December 2022, a major breach involving Maybank, the Election Commission (EC), and Astro Malaysia exposed the personal data of nearly 13 million account holders, including MyKad numbers, addresses, and mobile numbers. In the same year, WhatsApp reported that the mobile numbers of approximately 11.6 million Malaysian users were leaked as part of a global breach affecting 487 million accounts, while the EC's database was separately hacked, with sensitive voter details being sold for cryptocurrency. Similarly, AirAsia suffered a ransomware attack that compromised the data of five million passengers, and Carousell disclosed that 2.6 million users in Malaysia and Singapore had their personal details leaked due to a third-party system migration bug [3].

September 2022 alone saw two major breaches, the ePenyata Gaji system for civil servants, which exposed more than a million rows of personal and salary information, and Batik Air (formerly Malindo Air), where 45 million customer records, including passport numbers, were leaked. Other notable breaches included iPay88's compromise of customer card data in August 2022 and the National Registration Department (NRD) leak in May 2022, where a database of all Malaysians born between 1940 and 2004, amounting to 160GB of personal data, was allegedly offered for sale online. Earlier breaches also remain significant, such as the Facebook data leak in 2021 that exposed over 11 million Malaysians' details, Malaysia Airlines' Enrich frequent flyer programme breach covering a nine-year period, and the E-Pay Malaysia incident in which 380,000 customer records were sold on the dark web [3]. These recurring breaches reveal that the problem lies not only in technological vulnerabilities but also in governance, enforcement, and the lack of robust organizational compliance with statutory obligations.

The persistence of breaches despite statutory safeguards points to an institutional problem as many organizations fail to align their internal Standard Operating Procedures (SOPs) with PDPA

obligations. This misalignment creates gaps in enforcement, incident response, and staff training. Acknowledging these challenges, the government enacted the Personal Data Protection (Amendment) Act 2024 to be implemented in phases beginning in 2025. The amendments strengthen enforcement through higher penalties, extend obligations to data processors, and introduce new requirements such as mandatory Data Protection Officers and breach notifications. However, without effective organizational practices, these reforms risk remaining only on paper.

This situation raises a fundamental question as to what extent are consumer data breaches in Malaysia the result of legal deficiencies, as opposed to failures in implementation and corporate compliance? Addressing this question is crucial because consumer trust in digital ecosystems depends not only on strong legislation but also on effective execution. The objective of the study is to analyse why breaches persist despite the PDPA framework, to identify weaknesses in corporate SOPs and governance practices, and to propose recommendations to strengthen alignment between legal requirements and operational compliance. Ultimately, this study contributes to the broader discussion of how Malaysia can transition from a compliance-based approach to a trust-based data protection ecosystem, thereby enhancing both consumer confidence and the resilience of the digital economy.

2. Methodology

This research adopts a doctrinal and comparative legal research methodology supported by empirical content analysis of corporate privacy policies and secondary data on cybersecurity incidents. The study is designed to critically evaluate the adequacy of Malaysia's PDPA in addressing the rising trend of data breaches, with particular attention to enforcement challenges and corporate compliance practices. The doctrinal component involves a detailed examination of the statutory framework of the PDPA, including its seven Data Protection Principles, enforcement mechanisms, and penalty structure. Judicial decisions are analysed to determine how courts interpret and apply the Act in practice, particularly in relation to corporate standard operating procedures (SOPs) and consumer data protection. The study also examines relevant subsidiary legislation, guidelines issued by the Personal Data Protection Commissioner, and parliamentary debates to trace the legislative intent and policy objectives of the Act.

To place the Malaysian framework within an international context, the research conducts a comparative analysis of selected jurisdictions with mature data protection regimes, namely the European Union under the General Data Protection Regulation (GDPR) and Singapore under its Personal Data Protection Act 2012. These jurisdictions are chosen because they provide instructive models of breach notification regimes, higher penalty thresholds, and clear operational requirements for data subject rights. The comparison highlights best practices that could inform potential reforms to the Malaysian framework.

An empirical review of corporate privacy policies is conducted for seven Malaysian companies operating in key sectors, including real estate (Avaland Berhad), retail (Eco-Shop Marketing Sdn. Bhd.), manufacturing (Fumakilla Malaysia), oil and gas (PETRONAS), human resources (Peoplelogy Group), consumer goods (Sime Darby Berhad), and food and beverage (Loob Holding Sdn. Bhd.). Each privacy policy is analysed for its compliance with the PDPA's Notice and Choice Principle (Section 7), Disclosure Principle (Section 8), and Security Principle (Section 9). The analysis focuses on the clarity and specificity of consent mechanisms, the transparency of third-party disclosures, the level of detail regarding data retention periods, security safeguards, and procedures for data access and correction requests.

3. Literature Review

3.1 Legislative Framework of the PDPA

The PDPA, gazetted in 2010 and enforced in November 2013, designed to regulate the processing of personal data in commercial transactions [4]. Its primary purpose is to safeguard individuals against the misuse of their personal data by businesses and to ensure that such data is collected, stored and processed responsibly. By introducing clear obligations for data users, the PDPA aims to promote accountability and establish minimum standards for lawful data handling, thereby enhancing consumer trust in the digital economy.

Section 2 of the PDPA sets out the scope and applicability of the Act. Subsection (1) makes it clear that the Act applies not only to individuals or entities that directly process personal data but also those who exercise control over such processing or authorise it, provided the processing arises within the context of commercial transactions. This provision demonstrates the legislature's intention to regulate both the active data handlers of data and those occupying supervisory or authorizing roles.

Subsection (2) extends the applicability of the PDPA to two categories of persons. The first category comprises those established in Malaysia, regardless of whether the data is processed within or outside the country, either by the data user or through an appointed agent. The second category comprises those not established in Malaysia but who utilise equipment located in Malaysia to process personal data, except where such use is solely for transit purposes. This extraterritorial reach ensures that foreign entities cannot bypass Malaysian data protection obligations merely by operating from abroad while relying on local infrastructure to process personal data.

Subsection (3) further strengthens compliance by requiring foreign entities failing under subsection (2)(b) to appoint a representative who is established in Malaysia. This requirement is crucial as it ensures local accountability and facilities regulatory oversight, thus preventing enforcement gaps in relation to foreign data controllers or processors. Subsection (4) provides a detailed definition of what it means to be "established in Malaysia," a definition that is deliberately broad to prevent loopholes. It includes individuals present in Malaysia for at least 180 days in a calendar year, bodies incorporated under the Companies Act 1965, partnerships or unincorporated associations formed under Malaysian law; and any other persons maintaining an office, branch, agency, or regular practice within Malaysia. Through this comprehensive definition, the Act affirms its wide territorial scope and strengthens its regulatory reach over both domestic and foreign actors.

Section 5 of the PDPA sets out the obligation of every data user to comply with the Personal Data Protection Principles, which form the cornerstone of Malaysia's data protection framework. These principles cover the key aspects of data governance, including lawful processing, notice and choice, disclosure, security, retention, data integrity, and access rights. Together, they establish a legal framework that obliges data users to obtain consent before processing personal data, inform data subjects of the purposes of collection, restrict disclosure to authorised parties, secure the data against unauthorised access, retain it only for as long as necessary, ensure its accuracy and completeness, and provide data subjects with the right access and correct their data. Section 5 (2) further clarifies that any contravention of these principles constitutes an offence, subject to the provisions of sections 45 and 46 of the Act. The penalties for non-compliance are significant and include fines of up to RM300,000, imprisonment for a term not exceeding two years, or both. This combination of monetary and custodial sanctions reflects the seriousness with which the legislature views personal data protection and its intent to deter violations.

3.2 Weaknesses of the PDPA and Statistics in Data Breach Incidents

The PDPA prescribes a range of offences for non-compliance with its provisions, each carrying corresponding penalties. Among the most notable are offences for processing personal data in contravention of the Data Protection Principles, which is punishable by fines of up to RM300,000 or imprisonment of up to two years, or both. Similar penalties apply to the unlawful transfer of personal data outside Malaysia as per Section 129 of the PDPA, while more severe breaches such as processing data without a registration certificate under Section 16 or continuing to process data after registration has been revoked in Section 18, attract fines of up to RM500,000 and imprisonment of up to three years.

Section 108(8) address failures to comply with the directions or enforcement notices issued by the Commissioner, improper handling of sensitive personal data in Section 40(3), and refusal to cease processing upon withdrawal of consent in Section 38(4). These offences carry penalties ranging between RM100,000 and RM200,000 or imprisonment of up to two years, or both. Lesser penalties exist for obstruction of search under Section 120, unlawful tampering with sealed documents during search and seizure under Section 113(7), and breaches of confidentiality obligations under Section 141, which may carry fines as low as RM10,000 or imprisonment ranging from six months to one year. Additionally, the Act prescribes penalties of up to RM250,000 or imprisonment of up to two years, or both, for contraventions of specific regulatory requirements.

Despite this detailed framework, the PDPA is widely regarded as lenient and limited in scope. Its application is restricted to personal data processed in the context of commercial transactions, creating uncertainty as to whether individuals using social media for recreational purposes fall within its protection [5]. Furthermore, the Act does not explicitly cover the processing of employee data by employers, leaving a significant regulatory gap. These omissions are particularly concerning given the most internet users store and share personal information online, thereby heightening their exposure to cybersecurity threats. The increasing adoption of cloud-based services by both public and private sector organizations further amplifies the risk of unauthorized access and large-scale data breaches.

These regulatory gaps have contributed to Malaysia experiencing repeated and severe data breaches in recent years. Raj (2023) reports that Malaysia ranked as the eighth most breached country in Q3 2023, with nearly half a million leaked accounts [6]. The breach rate increased by 144% compared to the previous quarter, averaging four Malaysian user accounts leaked every minute. This highlights the vulnerability of personal data protection in the country.

The weaknesses of the PDPA have been further highlighted by major cybersecurity incidents over the past five years. In December 2022, hackers claimed to have obtained personal information belonging to 13 million voters from the Election Commission, as well as customer data from Maybank and Astro. Similarly, in November 2023, a hacker leaked a database of 487 million WhatsApp users worldwide, including 11 million Malaysian accounts. Other high-profile cases include the iPay88 data breach in May 2022, which potentially compromised customers' card details, and the alleged AirAsia ransomware attack in November 2022, which exposed data belonging to five million passengers and employees. Notably, September 2023 recorded the highest frequency of data breaches to date, averaging 15 reported cases per week, most of which involved ransomware attacks. These incidents demonstrate how insufficient legal safeguards, combined with inadequate enforcement, have enableed systemic cybersecurity vulnerabilities to persist [6].

To address these challenges, the Malaysian Computer Emergency Response Team (MyCERT) plays a key role as the national agency responsible for monitoring and responding to cybersecurity incidents. MyCert also publishes statistics and advisories, which serve as a primary reference for measuring the scale of cybersecurity threats in the country [7].

As of early 2025, Malaysia reported 34.9 million internet users, with 25.1 million social media users, representing 70.2 % of the total population. During the same period, the Federal Police Commercial Crime Investigation Department recorded a rise in online fraud cases between January and March 2025, surpassing the figures from previous quarter, which had already recorded 10,715 cases and financial losses amounting to RM519.9 million [8].

Data from Q2 2025 classify cybersecurity incidents into eight categories: fraud, intrusion, data breach, intrusion attempt, malicious code, spam, vulnerability report, and denial of service. Analysis of incidents in Q2 2025, as illustrated in Figures 1 and 2, reveals that fraud overwhelmingly dominates Malaysia's cybersecurity landscape, accounting for nearly four-fifths of all reported cases [8]. This concentration indicates that current preventative measures and enforcement under the PDPA are insufficient to deter fraudulent activity, particularly in financial transactions and online platforms where personal data is heavily utilised. The high prevalence of data breaches and intrusions further highlights systematic vulnerabilities in the way organisations secure and manage personal information.

Despite these alarming figures, the PDPA prescribes relatively modest penalties and remains limited in scope to commercial transactions, leaving significant gaps in protection for social media users and other non-commercial contexts. Malaysia's reliance on a narrow and lenient framework therefore undermines its capacity to address the escalating cyber threats reflected in the reported statistics, making legal reform both urgent and necessary.

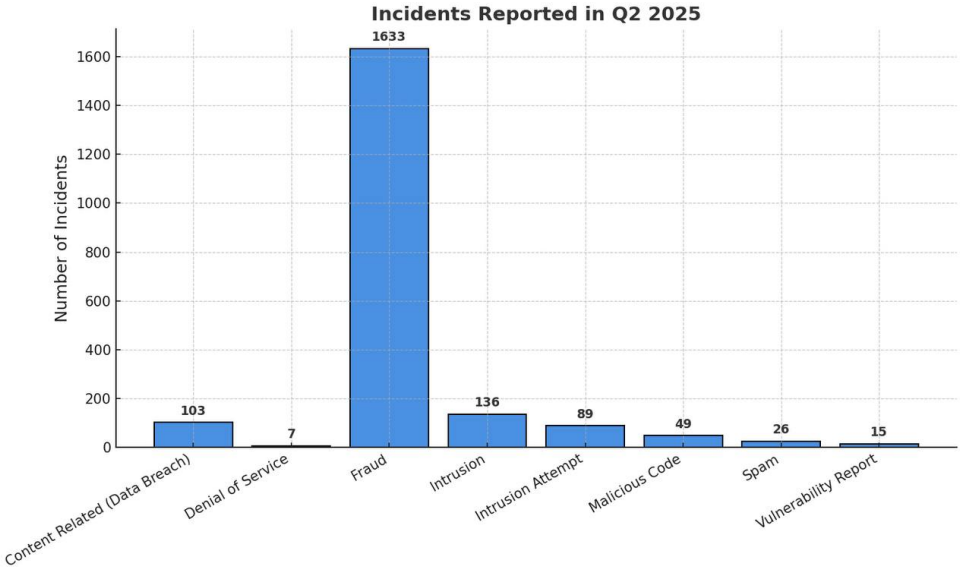


Fig. 1. Categorical distribution of incidents in Q2 2025

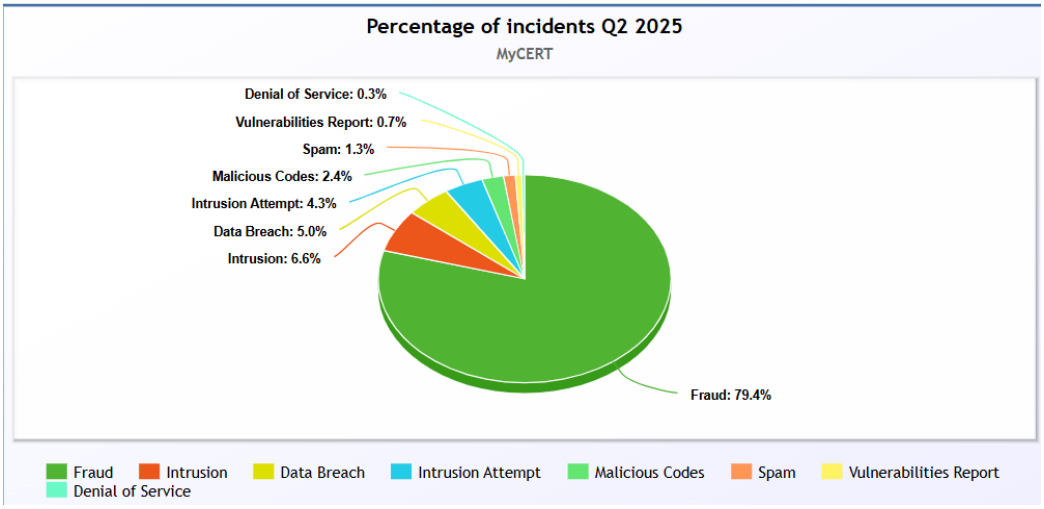


Fig. 2. Share of reported incidents by category in Q2 2025

3.3 Recorded Cybersecurity Incidents in Malaysia

The decision in *Public Bank Bhd v Tan Teck Seng Jason & Anor [2021] MLJU 92* [9], illustrates how the PDPA strengthens corporate standard operating procedures (SOPs) in safeguarding consumer data, even where such measures appear onerous to customers. The court upheld the bank's refusal to recognise an emailed request for change of address, reasoning that under Sections 36 and 37 of the PDPA, a data user is entitled to reject correction requests that lack adequate verification. By requiring biometric verification and written confirmation from all joint account holders, the bank's SOPs were fully aligned with the Security Principle under Section 9 of the PDPA, thereby minimising the risk of unauthorised access or fraudulent alteration of personal data. Although the Sessions Court had initially viewed this refusal as rigid and unfair to the consumer, the High Court rightly reframed the issue as consumer inconvenience cannot outweigh the statutory duty of a data user to maintain integrity and security of personal data. This reasoning demonstrates that corporate SOPs, when structured in accordance with statutory principles, do not merely shield corporations from liability but actively function as proactive mechanisms of consumer protection**.** In this way, the PDPA does not operate antagonistically to corporate operational procedures; rather, it legitimises and compels the design of robust verification mechanisms aimed at preventing the very misuse of data that the Act seeks to regulate.

Similarly, the 2021 case of *CIMB Bank Bhd v Roebuck Development [2021] MLJU 62* [10] highlights the PDPA's role in legitimising corporate non-disclosure as part of data protection SOPs. The plaintiff sought details of a third-party purchaser, but the court dismissed the application, holding that disclosure without consent would contravene Section 8 of the PDPA, which embodies the Disclosure Principle. By recognising the developer as a 'data user' bound by statutory confidentiality obligations, the court affirmed that corporate SOPs restricting disclosure are not merely internal policies, but legally enforceable duties. This reasoning demonstrates that the PDPA can operate as a shield against evidential demands in litigation, prioritising consumer privacy over corporate convenience or litigants' evidentiary needs. However, the case also exposes a tension: while non-disclosure prevents misuse of personal data, it can limit transparency and hinder a litigant's ability to prove claims. This judgement thus illustrates that the PDPA reshapes the relationship between data protection and procedural fairness by requiring corporations to structure their SOPs in a way that prioritises consumer privacy over adversarial demands for information.

3.4 Corporate Compliance Practices under the PDPA 2010

The Personal Data Protection Commissioner Office (PDPC) has issued guidelines to assist data users in forming comprehensive and reliable notices to ensure uniformity in handling consumer data across Malaysia. Section 7 of the PDPA 2010 imposes a statutory obligation on data users to provide a PDP Notice whenever they process personal data, regardless of the nature, form, or scale of their business operations. The PDP Notice functions as a formal written statement informing data subjects of the manner, purpose, PDP Notice serves solely as a notification tool and does not constitute a mechanism for obtaining consent to process personal data. Blanket consent clauses, whether embedded in the notice or in standard form contracts, do not satisfy the Act's requirement for valid consent. Instead, consent must be obtained separately, properly documented, and appropriately maintained by the data user as part of corporate governance and audit processes. This distinction highlights the PDPA's dual emphasis on transparency (through notice) and autonomy (through explicit consent), both of which are necessary to achieve effective consumer data protection [11].

The Act also prescribes mandatory elements that must be incorporated into every PDP Notice, including the purpose of data collection, the categories of data processed and the rights available to data subjects under the PDPA. Beyond these statutory requirements, best practice guidelines issued by the PDPC recommend that data users adopt notices that are clear, concise and accessible using plain language to facilitate comprehension. This approach ensures that data subjects are not merely informed in a formalistic sense but are able to understand the implication of data processing and exercise meaningful control over their personal information, consistent with the principle of informed consent [11].

The five key elements which must be reflected in the PDP Notice are as follows;

1. Personal data processed: The notice should specify the categories of personal data collected, including whether sensitive personal data or the data of minors under 18 years is processed.
2. Purpose and necessity of processing: The notice should identify the purposes for processing, disclose any regulatory requirements mandating such collection, state the retention period, and outline disposal procedures. It should also explain the practical measures taken to safeguard the data.
3. Source of personal data: The notice should indicate the internal and external sources from which data is obtained, such as manual registration forms or online portals.
4. Rights of data subjects: The notice must clarify whether providing data is mandatory or voluntary, and the consequences of refusal. It should explain how data subjects can access, correct, update, restrict, or withdraw consent to processing. Contact details of the officer responsible, including name, designation, phone number, and email, must also be provided for inquiries or complaints.
5. Disclosure to third parties: The notice should list the third parties to whom the data will be disclosed, explain the necessity of such disclosures, and outline the security measures in place to protect the data.

Transparency, accountability, and regular review are integral to the PDP Notice. Data users are legally required to provide full disclosure of all personal data processing activities, including activities such as contact tracing, the use of cookies, or the deployment of digital beacons. Importantly, data users must adhere strictly to the statements made in their PDP Notices; any deviation would amount to a breach of the Notice and Choice Principle as required in Section 7 of the PDPA. To maintain ongoing compliance, PDP Notices must undergo periodic review to reflect any changes in data processing practices, regulatory requirements or technological developments. Amendments must be

clearly documented and communicated to data subjects in a timely manner. Best practice further requires that notices specify key dates, including the date of issuance, the effective date, and the date of the recent review, to enhance transparency and enable data subjects to stay informed of the current terms under which their personal data is being processed [11].

To assess the feasibility of the PDPA, the Personal Data Protection (PDP) policies and notices of selected Malaysian companies will be examined. This analysis aims to evaluate how the provisions of the Act are operationalise in real corporate contexts. The companies chosen for review represent diverse sectors to ensure a broad perspective on compliance practices across different industries. A further criterion for selection is the public accessibility of their PDP Notice, which allows for transparent examination of the manner in which statutory requirements are translated into practice [11].

An analysis of the corporate privacy policies of seven Malaysian corporations, including Avaland Berhad, Sime Darby Berhad, Eco-Shop Marketing Sdn.Bhd., Fumakilla Malaysia, Petroliam Nasional Berhad (PETRONAS), Peoplelogy Group, and Loob Holding Sdn.Bhd., revealed a heterogeneous compliance landscape under the PDPA. Spanning sectors such as real estate, retail, manufacturing, oil and gas, consumer goods, human resources, and food and beverages, study shows that while these organizations demonstrate general adherence to the PDPA's core principles, significant variation exists in the depth, specificity, and transparency of their privacy practices. This disparity is not merely academic, as vague policies may undermine informed consent and expose individuals to risks of data misuse or breaches [11].

All seven corporations demonstrate a foundational commitment to the General Principle, particularly in obtaining consent for personal data processing. However, the methods for securing this consent vary from explicit acknowledgments, such as those used by PETRONAS, to implied consent inferred from a user's continued interaction with a service. This inconsistency suggests a potential gap in protecting individual autonomy, raising questions about whether implied consent truly aligns with the Act's intent. Similarly, adherence to the Notice and Choice Principle in Section 7 is widespread but the quality of notice differs markedly. Larger corporations such as Avaland and Sime Darby provide detailed PDP Notices, specifying categories of data collected, processing purposes, retention periods, and potential consequences of refusal. In contrast, smaller entities tend to issue generic minimalist notices, which may not sufficiently equip consumers to exercise meaningful choice. This pattern highlights a critical link between organisational capacity and the maturity of data governance frameworks, suggesting the resource-rich corporations are better positioned to operationalise comprehensive privacy management system [11].

A closer examination of the Disclosure Principle under Section 8 reveals a common recognition among corporations of the legal restrictions on third-party data sharing, yet there is a marked divergence in the degree of transparency with which this principle is implemented. While some companies such as Sime Darby and PETRONAS demonstrate good practices by specifying the categories of third parties with whom data may be shared. By contrast, several other corporations adopt vague and generalised language such as "third parties where necessary," a formulation that significantly limits the ability of data subjects to give truly informed consent. This lack of specificity represents a critical compliance gap, undermining both the Notice and Choice Principle and the broader objectives of data protection [11].

Furthermore, commitments relating to data security and retention are often framed in generic, non-specific terms. While larger corporations disclose detailed both technical and organisational measures, smaller companies typically provide only general assurances that data will be kept secure, leaving consumers without a clear understanding of the safeguards in place. The absence of specific retention periods or well-defined data destruction procedures in many policies further complicates

the matter, making it difficult for individuals to ascertain how long their personal data will be stored and whether it will eventually be securely disposed of [11]. The analysis also highlights systemic weaknesses in the operationalisation of data subject rights. While companies generally recognise individual rights to access and correct their personal data, they often fail to specify the procedures, timelines, or points of contact for exercising these rights. This omission diminishes the practical enforceability of statutory entitlements and risks rendering them largely symbolic. In contrast, corporations with more mature governance structures most notably PETRONAS and Sime Darby provide explicit, step-by-step procedures for data access and correction requests, contrasting sharply with the more limited commitments of smaller firms.

The Security Principle under Section 9 of the PDPA, which imposes an obligation on data users to take practical steps to protect personal data from loss, misuse, modification, or unauthorised access, is consistently acknowledged across all sampled companies in the study. However, the level of specificity and transparency in implementing this obligation varies considerably. Larger corporations, such as PETRONAS, Sime Darby, and Avaland, provide comprehensive descriptions of both their technical and organisational security measures. This suggests a more mature approach to personal data protection, likely attributable to their extensive resources, higher regulatory scrutiny. And the substantial volume of sensitive data under their stewardship [11].

In contrast, smaller entities such as Eco-Shop and Fumakilla rely on generic assurances that they take reasonable steps to secure personal data, without offering concrete details about the nature or scope of their security controls. This vagueness raises concerns regarding the actual implementation of these policies and weakens their enforceability, as general commitments may not translate into robust, demonstrable practices. The lack of specific detail in their policies may also make it more challenging for them to recover from a data breach as they may not have the necessary contingency plans in place [11].

Similarly, the Data Integrity Principle in Section 11, which requires data users to take reasonable steps to ensure accuracy and completeness, is addressed with varying degrees of success. Larger corporations, including Sime Darby and PETRONAS, have established clear procedures for individuals to update their personal data, ensuring its accuracy over time. This proactive approach is a hallmark of strong corporate governance and fosters greater consumer privacy. Conversely, smaller companies like Eco-Shop merely acknowledge the right to request corrections without outlining the specific internal processes for doing so. This procedural gap suggests that while the principle is recognized on paper, it may not be fully operationalized, creating a potential barrier for data subjects seeking to correct inaccuracies. The varying approaches to these two principles underscore a key finding of the study: compliance maturity is often correlated with the size and resource capacity of the organization [11].

Previous scholarly work on Malaysian privacy policies, such as the 2017 study by Chua [12], established a persistent gap between formal compliance with the PDPA and the Act's underlying objective of meaningful consumer protection. While certain sectors, particularly those entrusted with sensitive data such as banking, healthcare and telecommunications, demonstrate higher levels of PDPA compliance, most organisations still fail to meet the full spectrum of statutory requirements. Notably, Chua research identifies an inverse relationship between policy readability and compliance, suggesting that simpler, more concise policies often omit crucial provisions for personal data protection, whereas more legally comprehensive documents are frequently complex and difficult for the average consumer to understand.

Overall, the findings suggest a regulatory paradox, where efforts to make privacy policies consumer-friendly may inadvertently dilute their protective effect. To truly bolster consumer privacy, regulatory intervention may be needed to mandate (1) clear and specify third-party disclosure

requirements, ensuring datae subjects understand with whom their data is shared, (2) defined timelines for fulfilling data access and correction requests, thereby operationalising individual rights and (3) periodically review and update obligations for corporate privacy policies, including the requirement to display effective dates and revision histories, ensuring continued relevance in a rapidly evolving digital environment. Such measures would not only strengthen substantive compliance but also cultivate a culture of accountability and transparency, ultimately advancing the PDPA's objective of safeguarding personal data in Malaysia's increasingly data-driven economy [12].

3.5 Comparative Analysis of Malaysia's PDPA 2010 with Singapore's Personal Data Protection (Amendment) Act (SPDPA) 2020 and General Data Protection Regulation (GDPR) by European Union (EU)

Malaysia's PDPA marked a significant step toward safeguarding personal information, yet its scope and enforcement mechanisms have often been criticized as limited in ambition and effectiveness. To assess the strength of Malaysia's framework, this study adopts a doctrinal and functional comparative approach, analysing not only statutory provisions but also how different regimes address similar regulatory challenges in practice.

Two jurisdictions are selected for comparison, namely the European Union (EU) and Singapore. The EU's General Data Protection Regulation (GDPR) is widely regarded as the global "gold standard," offering a comprehensive rights framework, extraterritorial reach, and stringent enforcement mechanisms. Singapore's Personal Data Protection Act 2012 (amended 2020), by contrast, reflects a pragmatic regional model, balancing regulatory oversight with business innovation while sharing Malaysia's common law heritage and comparable economic profile

To effectively evaluate the Malaysian PDPA 2010, this analysis employs a comparative approach by examining two key international regulatory frameworks: the European Union's GDPR and Singapore's PDPA 2020. The GDPR was chosen for its status as a global benchmark for consumer privacy, widely considered the most stringent and comprehensive data protection regime. Its influence has extended far beyond Europe, shaping legislative reforms worldwide through its focus on data subject rights, accountability, and its broad extraterritorial reach. Meanwhile, Singapore provides a highly relevant regional comparator. Sharing a common law heritage with Malaysia and navigating similar technological and economic landscapes, Singapore's framework offers a pragmatic model that balances the protection of personal data with the promotion of digital innovation. Noteworthy features of the Singaporean legislation include its data portability rights and enhanced penalties, which offer valuable insights into potential regulatory improvements. By juxtaposing the Malaysian PDPA against the rigorous, rights-driven framework of the GDPR and the regionally adapted, business-friendly approach of Singapore, this study not only clarifies Malaysia's current position in the international landscape of corporate governance but also highlights practical avenues for future reform within the ASEAN context.

3.5.1 Scope of protection

The scope of Malaysia's PDPA 2010 is notably more limited than its international counterparts, a restriction that impacts consumer privacy. As specified in Section 2(1), the Act's application is explicitly confined to "personal data in respect of commercial transactions," a narrow definition that excludes data processed by the government and for non-commercial purposes. In contrast, Singapore's PDPA 2020, under Section 4(1), applies broadly to all organizations, with exemptions only for public agencies and personal use as outlined in Section 4(2). While this governmental exclusion is

like Malaysia's, Singapore's framework is far more comprehensive in its coverage of the private sector.

The most extensive scope is found in the European Union's General Data Protection Regulation (GDPR). According to Article 2(1), the GDPR applies to any processing of personal data by automated or structured means, with limited exceptions under Article 2(2) for household or national security purposes. Additionally, Article 3 gives the GDPR extraterritorial reach, significantly extending its protective scope. The GDPR also adopts a broader definition of personal data as highlighted by Von dem Bussche [13], the mere possibility of identification, such as through the combination of various data points, is sufficient for data to be considered personal under Article 4 No. 1. This is a far cry from the Malaysian PDPA, whose restricted scope appears outdated given the nature of the modern digital economy where personal data often transcends commercial classifications.

A prior study conducted by Zulhuda [14] on data protection in the Internet of Things (IoT) era suggests that the current protections afforded by the Malaysian PDPA 2010 are insufficient for this environment. The study attributes this inadequacy to two primary factors. The first is the narrow scope of the Act, which, as previously discussed, is limited to personal data processed solely within commercial transactions. The second factor is the Act's inability to keep pace with the rapid technological advancements in data processing. These findings emphasise a critical gap in Malaysia's corporate governance framework for personal data protection, particularly as data breaches in an IoT context can have widespread and severe consequences for consumer privacy.

3.5.2 Extraterritorial application

An important limitation of Malaysia's PDPA 2010 is its lack of extraterritorial application, which leaves citizens vulnerable when their personal data is processed by foreign entities outside the country's borders. This is a critical deficiency in the context of globalized data flows, as noted by Alibeigi and Munir [15], who point out that the PDPA does not apply to data belonging to Malaysians when it is processed and used abroad. They suggest that future amendments should explicitly include "personal data of Malaysians" under Section 3(2) and address the imprecision of the term "intended" in relation to data processing in Malaysia. In contrast, SPDPA provides a degree of cross-border protection, which restricts data transfers to jurisdictions that offer a comparable level of personal data protection. Ee-Ing Ong [16] further clarifies that Singapore's regulatory framework can extend to non-Singaporean organisations as long as the data is located within its territory, and the country's Computer Misuse and Cybersecurity Act asserts extraterritorial jurisdiction over actions that cause significant harm within Singapore.

The GDPR sets an even more rigorous benchmark for extraterritorial application. Article 3(2) of the GDPR extends its reach to any non-EU controller or processor that offers goods or services to EU residents or monitors their behavior, a groundbreaking provision that effectively exports EU consumer privacy standards globally. While the GDPR's extraterritoriality has been subject to legal interpretation, as Kuner [17] highlights, its application is generally limited to specific circumstances and does not extend to subjects of international law, such as international organisations. Nevertheless, the stark contrast in these approaches underscores Malaysia's more insular legal framework, which hinders strong corporate governance and personal data protection in the digital economy.

4. Results and Recommendations

The analysis of Malaysia's PDPA and related corporate practices demonstrates that persistent data breaches in the country stem from both legislative limitations and weaknesses in organizational implementation.

First, the scope of protection under the PDPA remains narrow, applying mainly to personal data processed in commercial transactions. This leaves significant categories of personal data, such as those processed in social media contexts and employment relationships, beyond its coverage. As a result, many individuals remain exposed to privacy risks in increasingly digital and interconnected settings [4].

Second, enforcement mechanisms under the PDPA are relatively weak. While offences and penalties are provided under the Act, they are comparatively lenient when measured against international benchmarks such as the GDPR. The absence of mandatory breach notifications, limited investigatory powers, and modest fines reduce the law's deterrent effect [5].

Third, corporate compliance practices were found to be inconsistent across organizations. While most companies publish PDP Notices, their quality and detail vary significantly. Larger corporations tend to provide more comprehensive disclosures and security measures, whereas smaller entities rely on vague and general statements. Similarly, approaches to securing consent, data retention, and access rights are uneven, leading to gaps in transparency and accountability [11].

Judicial decisions such as *Public Bank Bhd v Tan Teck Seng Jason [2021] MLJU 92* and *CIMB Bank v Roebuck Development [2021] MLJU 62* confirm that corporate SOPs are aligned with the PDPA can effectively strengthen consumer protection. However, the inconsistent adoption of robust SOPs across industries suggests that enforcement and monitoring are inadequate.

Finally, comparative analysis with SPDPA 2020 [16] and the EU's GDPR [13,17] highlights Malaysia's shortcomings in areas such as extraterritorial application, data subject rights, and breach notification requirements. These gaps reduce Malaysia's resilience against transnational cyberthreats and limit its alignment with global standards of consumer data protection.

In view of these findings, several measures are recommended to strengthen Malaysia's data protection framework and enhance consumer trust. First and foremost, it is imperative to strengthen the legal framework by expanding the scope of the PDPA beyond commercial transactions, so that personal data processed in non-commercial contexts such as social media and employment is also protected. At the same time, the penalty structure should be revised to reflect international standards, particularly those of the GDPR, so that sanctions serve as an effective deterrent rather than a modest inconvenience. The enforcement powers of the Personal Data Protection Commissioner should also be enhanced to include real-time monitoring, mandatory breach notification, and public reporting of enforcement actions.

Equally important is the need to improve corporate governance. Organizations must embed data protection obligations into their internal culture through the institutionalisation of clear and dynamic SOPs. This involves regular training for staff, the conduct of compliance audits, and the implementation of breach simulation exercises to ensure preparedness against evolving cyberthreats. In this regard, data protection must be treated not merely as a statutory obligation but as a fundamental component of corporate accountability.

Transparency and consumer rights also require further attention. PDP Notice should be standardised across industries to ensure clarity and accessibility for consumers, while additional rights such as the right to access, rectify, or erase personal data, should be introduced to empower individuals in line with international best practices. Furthermore, independent channels for

complaints and redress should be established to provide consumers with reliable avenues of protection beyond corporate mechanisms.

Finally, Malaysia must recognise the cross-border nature of cyberthreats and foster greater collaboration both domestically and internationally. Stronger partnerships between the PDPC, MyCERT, law enforcement, and financial regulators will enhance enforcement at the national level, while cooperation with regional and global regulators will facilitate more effective responses to transnational breaches. Through such an integrated approach, Malaysia can bridge the gap between law and practice, ensuring that personal data protection evolves into a culture of accountability that supports long-term trust and sustainability in the digital economy.

5. Conclusions

This research finds that persistence of large-scale data breaches in Malaysia is driven less by the absence of a legal framework and more by weak regulatory enforcement and inconsistent corporate compliance [4]. Although the PDPA establishes a foundational structure for safeguarding personal data, its narrow scope [14], limited to commercial transactions, combined with modest statutory penalties and the absence of a mandatory data breach notification regime [5] significantly undermine its effectiveness. The analysis further reveals that corporate SOPs, while generally aligned with the PDPA's principles, often lack the depth, transparency and operational rigor necessary to provide meaningful protection for data subjects. This gap between formal compliance and substantive protection exposes individuals to ongoing risks, eroding public trust in Malaysia's data protection regime [6]. Comparative insights from the GDPR [13,17] and SPDPA [16] show the importance of expanding legal coverage to include non-commercial contexts, such as social media and employee data, introducing stricter sanctions that are proportionate to the harm caused by data breaches and mandating breach notifications and establishing clear timelines for data subject rights enforcement. Strengthening both regulatory enforcement and corporate governance is therefore essential to restore public confidence, ensuring accountability, and building a resilient data protection ecosystem capable of supporting Malaysia's ambitions for a trusted, secure and sustainable digital economy.

Acknowledgement

This research was not funded by any grant.

References

[1] Aliza Shah and Iylia Marsya Iskandar. "'15 Data Breach Cases per Week' [NSTTV]: New Straits Times." NST Online, September 21, 2023. https://www.nst.com.my/news/nation/2023/09/957822/15-data-breach-cases-week-nsttv.
[2] "Cyber Security Breaches." DataGuard, March 8, 2023. https://www.dataguard.com/cyber-security/breaches/.
[3] Loheswar, R. "Major Data Breaches in Malaysia in the Past 24 Months." Malay Mail, December 31, 2022. https://www.malaymail.com/news/malaysia/2022/12/31/major-data-breaches-in-malaysia-in-the-past-24-months/47722.
[4] Personal Data Protection Act 2010 (Act 709), Sections 2(1)–(4), 5, 5(2), 6–12, 16, 18, 38(4), 40(3), 45, 46, 108(8), 113(7), 120, 129, 141.
[5] Leng, Olivia Tan Swee, Rossanne Gale Vergara, and Shereen Khan. "Digital tracing and Malaysia's personal data protection act 2010 amid the COVID-19 pandemic." (2021).https://doi.org/10.33093/ajlp.2021.3
[6] Raj, Aaron. 2024. "Malaysian Telco Provider Has Data Breach – Again." Tech Wire Asia, January 30, 2024. https://techwireasia.com/2024/01/malaysian-telco-provider-has-data-breach-again/
[7] MyCERT, 'About us' https://www.mycert.org.my/portal/full?id=d8032294-04b2-4ba0-9e46-62c898bb4983
[8] MyCERT, Cyber Incident Quarterly Summary Report – Q2 2025 (SR-031.082025). CyberSecurity Malaysia. August 6, 2025. https://mycert.org.my/portal/advisory?id=SR-031.082025
[9] *Public Bank Bhd v Tan Teck Seng Jason & Anor* [2021] MLJU 92

[10] *CIMB Bank Bhd v Roebuck Development Sdn Bhd* [2021] MLJU 62
[11] Personal Data Protection Commissioner. *Guidance on the Preparation of Personal Data Protection Notices*. 2024. Accessed September 24, 2025. https://www.pdp.gov.my/ppdpv1/en/akta/guidance-on-the-preparation-of-personal-data-protection-notices/
[12] Chua, Hui Na, Anthony Herbland, Siew Fan Wong, and Younghoon Chang. "Compliance to personal data protection principles: A study of how organizations frame privacy policy notices." *Telematics and Informatics* 34, no. 4 (2017): 157-170.https://doi.org/10.1016/j.tele.2017.01.008
[13] Voigt, Paul, and Axel Von dem Bussche. "The eu general data protection regulation (gdpr)." *A practical guide, 1st ed., Cham: Springer International Publishing* 10, no. 3152676 (2017): 10-5555.https://doi.org/10.1007/978-3-319-57959-7
[14] Sidi Ahmed, Sidi Mohamed, and Sonny Zulhuda. "Data protection challenges in the internet of things era: an assessment of protection offered by PDPA 2010." *International Journal of Law, Government and Communication (IJLGC)* 4, no. 17 (2019). https://doi.org/10.35631/ijlgc.417001
[15] Alibeigi, Ali, and Abu Bakar Munir. "Malaysian personal data protection act, a mysterious application." *U. Bologna L. Rev.* 5 (2020): 362.https://doi.org/10.6092/issn.2531-6133/12441
[16] ONG, Ee-Ing. "Data protection in the Internet: National rapporteur (Singapore)." (2018). https://doi.org/10.1007/978-3-030-28049-9_13
[17] Kuner, Christopher. "The GDPR and international organizations." (2020): 15-19.https://doi.org/10.1017/aju.2019.78