INTERNATIONAL JOURNAL OF ACADEMIC RESEARCH IN BUSINESS & SOCIAL SCIENCES

Vol 15, Issue 12, (2025) E-ISSN: 2222-6990

E-Commerce and Data Protection Laws: A Comparative Study of Malaysia, Singapore, and Australia

Iyllyana Che Rosli[1]*, Kirtisha Siva[1], Fadiah Hanis Wahida Rosdilah[1], Tengku Chik Abu Bakar Tengku Ibrahim[2] and Mohamad Nurul Hafiz Ab Latif[3]

[1]Law Department, Faculty of Law and International Relations, (UniSZA), Gong Badak Campus, 21300, Kuala Nerus, Terengganu, Malaysia, [2]Law Department, School of Law, Politics and Sociology, University of Sussex, BN19RH Brighton, United Kingdom, [3]Department of Da'wah and Islamic Civilization, Faculty of Islamic Contemporary Studies, Universiti Sultan Zainal Abidin (UniSZA), Gong Badak Campus, 21300, Kuala Nerus, Terengganu, Malaysia

*Corresponding Author Email**:** iyllyanarosli@unisza.edu.my

DOI Link: http://dx.doi.org/10.6007/IJARBSS/v15-i12/27136

Published Date: 17 December 2025

Abstract

The increasing use of e-commerce in Malaysia, Singapore, and Australia has broadened the volume and types of personal data processed by online platforms, prompting closer attention to data protection frameworks. This study conducts a doctrinal and comparative analysis of the principal laws governing personal data protection in e-commerce across the three jurisdictions, including recent developments in Malaysia such as the introduction of mandatory personal data breach notification under Section 12B of the Personal Data Protection Act 2010 and the issuance of the 2025 Data Breach Notification Guideline. The research examines statutory requirements, regulatory structures, and procedural obligations to address three questions: the legal frameworks applicable to data protection in e-commerce; main divergence among Malaysia, Singapore, and Australia; and potential recommendations Malaysia may consider as its framework evolves. The findings indicate that although the jurisdictions share core data protection principles, differences arise in enforcement approaches, scope, governance mechanisms, and the management of sensitive information. Malaysia's recent amendments reflect an expanding regulatory framework that introduces more structured breach notification and accountability processes. The comparative observations provide insight into how the three jurisdictions address similar regulatory challenges and may inform Malaysia's ongoing regulatory development in the context of its growing digital economy.

Keywords: E-commerce, Data Protection, Malaysia, Singapore, Australia

Introduction

The rapid expansion of e-commerce has fundamentally transformed how individuals purchase goods, access services, and participate in the digital economy. E-commerce broadly refers to commercial transactions conducted wholly or partly through electronic means, encompassing the buying, selling, and exchange of goods, services, or information via computer networks, particularly the internet (Sirurmath & Pani, 2004) It spans a wide range of activities, including retail transactions, online marketplaces, auctions, and inter-business exchanges , and operates across multiple transactional models such as Business-to-Consumer (B2C), Business-to-Business (B2B), Consumer-to-Consumer (C2C), and Business-to-Government (B2G) arrangements (Begum & Kavitha, 2023).

As commercial activity increasingly migrates to digital platforms, vast amounts of personal data including names, contact details, financial information, and behavioural patterns are routinely collected, processed, and transferred. While this shift has improved consumer convenience and facilitated business innovation, it has simultaneously intensified concerns regarding privacy, data security, and the adequacy of legal safeguards governing digital interactions (Pregoner et al., 2020; Rajkumar et al., 2024). These concerns are particularly acute in jurisdictions experiencing rapid digitalisation, where regulatory frameworks must evolve alongside technological and commercial change.

In Malaysia, the growth of e-commerce accelerated significantly during the COVID-19 pandemic, as consumers increasingly relied on online platforms for safety and convenience (Nadzri et al., 2023; Seah et al., 2022). Empirical evidence indicates that online retail sales increased by 28.9% in April 2020 (A. Mohamad et al., 2025)compared to the same month in the previous year reflecting a significant shift in consumer purchasing behaviour driven by restrictions on physical movement (Aryani et al., 2021). However, this rapid expansion has also exposed vulnerabilities within the digital marketplace. The widespread use of platforms such as Shopee, Lazada, Grab, and Shein has been accompanied by rising reports of data breaches, consumer complaints, and online fraud (A. Mohamad et al., 2025). Notably, cases of e-commerce-related fraud in Malaysia increased by over 173% between 2019 and 2021, highlighting the heightened risks associated with intensified online transactions (Z. Mohamad et al., 2023; Noor et al., 2022).

Against this backdrop, the adequacy of Malaysia's legal framework for personal data protection in e-commerce merits closer examination in light of comparative regulatory developments. Personal data protection in Malaysia is primarily governed by the Personal Data Protection Act 2010 (PDPA 2010), which establishes seven core principles relating to consent, notice, disclosure, security, retention, data integrity, and access (Kamaruddin et al., 2025). These principles set baseline obligations for organisations engaged in commercial data processing and are supplemented by the Personal Data Protection Regulations 2013 and Data Protection Standards 2015. The broader regulatory environment further includes statutes such as the Consumer Protection Act 1999, Digital Signature Act 1997, and Computer Crimes Act 1997, which collectively address consumer rights, authentication mechanisms, and cybercrime risks in online transactions.

Recent developments have strengthened Malaysia's framework through the introduction of mandatory data breach notification under Section 12B of the PDPA 2010, supported by the

Data Breach Notification Guideline (2025) (Kennedy et al., 2025). This regime requires data controllers to notify the Personal Data Protection Commissioner within 72 hours of becoming aware of a breach and to inform affected individuals within seven days where significant harm is likely. While these reforms represent meaningful progress, they also highlight the continuing need to assess whether Malaysia's framework is sufficiently comprehensive, particularly when measured against more mature regulatory regimes (Prasetyoningsih et al., 2024)..

In this respect, comparative insights from Singapore and Australia are especially valuable. Both jurisdictions regulate personal data through well-established statutory frameworks, i.e. the Singapore Personal Data Protection Act 2012 and the Australia Privacy Act 1988, in which both jurisdictions incorporate breach notification requirements, governance obligations, and robust enforcement mechanisms. Differences in regulatory design, institutional capacity, and policy priorities across these jurisdictions provide a useful lens through which to evaluate Malaysia's evolving approach to data protection. Against this contextual and comparative background, this paper examines the regulation of personal data arising from e-commerce activities and considers how Malaysia might further strengthen its legal framework. Adopting doctrinal and comparative law analysis, the paper addresses three research questions: (i) What laws govern data protection in e-commerce in Malaysia, Singapore, and Australia?; (ii) How do these regulatory frameworks differ?; and (iii) What improvements could be considered to enhance Malaysia's framework? The scholarly contribution of this study lies in its combined doctrinal and comparative analysis of data protection in the e-commerce context, with particular emphasis on recent legislative developments such as mandatory breach notification and cross-border data governance. By systematically comparing Malaysia's framework with those of Singapore and Australia, the paper offers original insights into regulatory divergences and convergence within the Asia–Pacific region and advances practical recommendations to support Malaysia's ongoing efforts to strengthen its data protection regime in the digital economy.

Literature Review

The Growth of E-Commerce and Data Protection Challenges

E-commerce has become a central feature of modern commercial activity, supported by the widespread adoption of digital platforms and increased consumer reliance on online transactions (Marx & Niasin, 2023). Academic literature highlights that e-commerce generates significant volumes of personal data, ranging from basic identifiers to sensitive financial and behavioural information (Begum & Kavitha, 2023; Jeyapriya et al., 2019). As transactions expand across B2C, B2B, C2C and B2G channels, the exposure of personal data to cybersecurity risks grows correspondingly. E-commerce platforms are increasingly targeted by cyber-attacks such as malware, Distributed Denial-of-Service (DDoS) attacks, social engineering, and data breaches, which jeopardize user privacy and platform security (Udayaprasad et al., 2025). Data breaches, inadequate privacy practices, and evolving cybersecurity threats continue to affect how e-commerce platforms handle consumer information (Mannan, 2024). The misuse of personal data by companies without customer consent further exacerbates privacy concerns (Channak et al., 2023). As the digital marketplace expands, the protection of consumers' personal data becomes increasingly vital to foster trust and encourage participation in online transactions.

The rise of e-commerce in Malaysia has been marked by rapid expansion driven by technological advancements and evolving consumer behaviour (Kiu & Lee, 2017). High smartphone penetration and wider internet access have enabled seamless participation in digital marketplaces. This growth was further accelerated by the COVID-19 pandemic, which prompted significant shifts in purchasing patterns and encouraged businesses to adopt digital platforms to maintain continuity (A. Mohamad et al., 2025). The existing legal framework, led by the PDPA 2010, serves as the cornerstone for personal data rights in Malaysia. However, the PDPA 2010 faces substantial challenges in keeping pace with the accelerating e-commerce landscape (Alibeigi & Munir, 2020; Kamaruddin et al., 2025; Prasetyoningsih et al., 2024). These developments have prompted renewed scholarly interest in assessing the robustness of Malaysia's legal framework and its ability to address emerging privacy and security risks within digital commerce.

Legal Framework on Data Protection in Malaysia

Malaysia's principal legislation governing personal data is the PDPA 2010, which applies to data processed in commercial transactions. PDPA 2010 is recognised as a significant milestone in Malaysian privacy regulation, introducing seven core principles relating to consent, notice, disclosure, security, retention, integrity, and access (Ismail, 2012; Kamaruddin et al., 2025; Prasetyoningsih et al., 2024). This legislation represents a comprehensive legal framework designed to protect the personal data of individuals and regulates the collection, processing, use, and disclosure of personal data in consumer and business contexts (Razali et al., 2022). The PDPA 2010 delineates specific responsibilities for data users, requiring them to obtain consent from individuals before processing their data and to ensure that the data collected is securely stored and not misused (Sholehuddin et al., 2024). One of the main principles of the PDPA 2010 is the requirement for transparency in data processing activities. Organisations are obligated to inform individuals about the purposes for which their data is being collected, used, and shared. This requirement serves to enhance accountability and establish trust between consumers and e-commerce platforms (A. Mohamad et al., 2025). The general principle also prohibits the processing of any data, unless it is for a lawful purpose directly related to the activity of the data user as it also has been mentioned under Section 6(3) of the Act. For sensitive personal data, such as information about physical or mental health, political opinions or religious beliefs, explicit consent be obtained before processing. Furthermore, the PDPA 2010 mandates that data users implement appropriate security measures to protect personal data from unauthorised access or breaches, ensuring a robust level of data protection during e-commerce transactions (Sholehuddin et al., 2024). This principle required data user to inform the person in writing and to provide an outline of the data that relates to the individual concerned. It also stated under Section 31 (2) of the Act as the compliance with data access request which it must be request within the period of twenty-one days from the date of receipt. Consumers have the right to access their personal data and request corrections, which empowers them to control their information and enhances trust in e-commerce platforms (Alibeigi et al., 2021).

Beyond the PDPA 2010, Malaysia's data protection landscape in e-commerce is supported by several complementary statutes. The Digital Signature Act 1997 (DSA 1997) provides the legal basis for recognising digital signatures as valid and enforceable electronic signatures in commercial transactions. It regulates certification authorities, mandates licensing and oversight, and imposes duties on subscribers to provide accurate information and safeguard

their private keys. By linking cryptographic techniques to statutory rules on authenticity, non-repudiation and security, the DSA 1997 strengthens trust in electronic communications and online transactions. The Consumer Protection Act 1999 (CPA 1999), together with the Consumer Protection (Electronic Trade Transactions) Regulations 2012, protects e-consumers through provisions on misleading representations, unfair terms, accurate pricing and transparent online disclosures (Narayanasamy et al., 2017). Although the PDPA 2010 directly governs personal data processing, the CPA 1999 reinforces data protection indirectly by requiring fair dealing and informed consent in e-commerce transactions, with enforcement supported by the Ministry of Domestic Trade and Consumer Affairs and the Tribunal for Consumer Claims. In parallel, the Computer Crimes Act 1997 (CCA 1997) addresses unauthorised access, hacking, data theft and related cyber offences, thereby securing the technological environment within which personal data is processed. Its focus on criminal liability for unauthorised access and misuse of computer systems complements the PDPA's civil-regulatory model and aligns with broader constitutional recognition of privacy interests (Yeon et al., 2022). These acts collectively address various aspects of data protection, from secure digital signatures to consumer rights and cybercrime prevention, ensuring a safer online environment for all stakeholders.

The PDPA has been criticised for its relatively narrow scope, particularly due to its exclusion of Federal and State Governments and certain categories of data processing activities (Kamaruddin et al., 2025). These exemptions, together with limited enforcement mechanisms, have raised concerns that the framework may not provide sufficiently comprehensive protection in an increasingly complex digital environment (Alibeigi & Munir, 2020). Comparing the PDPA 2010 with international standards like the EU's General Data Protection Regulation (GDPR), while Malaysia's PDPA adopts some principles from the GDPR, it falls short in several areas, including the protection from automated decision-making and the need for a more robust enforcement mechanism (Pour, 2025; Shahul Ikram, 2024).

Legal Framework on Data Protection in Singapore

Singapore has established a comprehensive and structured regulatory regime for personal data protection, designed to balance the needs of a rapidly expanding digital economy with the imperative to safeguard individual privacy. At the centre of this framework is the Personal Data Protection Act 2012 (PDPA 2012), which governs the collection, use, disclosure, and management of personal data by private sector organisations. The PDPA reflects Singapore's policy objective of supporting business innovation while ensuring responsible data-handling practices, making it a key pillar of regulatory governance for e-commerce and digital transactions.

A core component of Singapore's PDPA 2012 is its emphasis on organisational accountability, requiring entities to appoint one or more individuals to oversee compliance functions. Under Section 11(3), organisations must designate personnel responsible for implementing internal policies and ensuring adherence to statutory obligations. The Act also embeds consent-based processing, mandating that organisations obtain clear consent from individuals before collecting, using, or disclosing personal data (Goh, 2018). Sections 13–17 provide detailed rules on valid consent, including circumstances in which consent is deemed invalid, such as when individuals have not been properly informed of the purposes of collection. These provisions collectively enhance transparency and reinforce public trust in digital transactions.

The PDPA 2012 further incorporates purpose limitation and data accuracy obligations, ensuring that organisations process personal data only for purposes a reasonable person would consider appropriate in the circumstances (Section 18) and that data used to make decisions affecting individuals is accurate and complete (Section 23). The PDPA 2012 grants individuals' rights regarding their data. They have the right to access their personal data held by organizations, as well as the right to request corrections if necessary(Fauzi & Andriasari, 2025). The legislation stipulates that personal data should only be retained as long as necessary for fulfilling its intended purpose. After that period, organizations must dispose of the data securely(Kamila et al., 2025). This aspect is particularly relevant in the context of e-commerce, where sensitive information, such as payment details, is frequently processed(Raghavan et al., 2021). The Act also regulates cross-border data transfers, restricting such transfers unless the receiving jurisdiction provides comparable protection or an exemption is approved by the Personal Data Protection Commission (PDPC). The PDPC has the authority to impose fines and penalties for non-compliance, thereby providing a layer of accountability within the framework(Soemitro et al., 2023).

Case law has supported the development of Singapore's data protection jurisprudence. In *Michael Reed v Alex Bellingham*, the Court of Appeal examined whether emotional distress and loss of control over personal data could constitute "loss or damage" under Section 32(1), reinforcing the centrality of consent and fair processing within the PDPA 2012. Singapore has also expanded its regulatory ecosystem through instruments such as the Do Not Call (DNC) Registry under Part XI of the PDPA 2012, which allows individuals to opt out of telemarketing communications and obliges organisations to check the registry prior to sending marketing messages. Collectively, these legislative and jurisprudential elements illustrate Singapore's robust and evolving data protection landscape, providing a mature model within the Asia-Pacific region for managing personal data in the context of e-commerce.

Legal Framework on Data Protection in Australia

Australia's regulatory approach to personal data protection in e-commerce is primarily structured around the Privacy Act 1988, which establishes the overarching principles and obligations governing the handling of personal information (Waters, 2012). Central to this Act are the Australian Privacy Principles (APPs), which set standards for the collection, use, disclosure, and secure storage of personal information by organisations and federal agencies (Patro et al., 2016). It aims to protect individuals' privacy and includes principles for the collection, use, and disclosure of personal data(Zulham, 2023). The Act applies across the Commonwealth, its states, territories, and extended territories, ensuring broad coverage across both public and private sectors. Under this framework, individuals retain the right to control the flow of their personal data, reflecting Australia's emphasis on balancing privacy with other competing societal interests. A key element of Australia's privacy regulation lies in the definition and treatment of sensitive information, which includes data that can identify an individual, such as full name, date of birth, or gender (Kemp, 2022). The Act also requires that consent, whether express or implied shall be fully informed, specific, current, and given by someone with capacity. Australia's privacy protection operates through a combination of statutory regulation and common law, complemented by industry self-regulation. While the Federal Privacy Act governs public agencies, the Privacy Amendment (Private Sector) Act 2000 extends coverage to the private sector's handling of personal data. These legislative layers aim to promote transparency and accountability in data governance.

Enforcement of the Privacy Act is vested in the Office of the Australian Information Commissioner (OAIC), which plays a pivotal role in monitoring compliance, conducting investigations, issuing enforcement undertakings, and providing public guidance on privacy matters(Kemp, 2022). The OAIC is empowered to audit organisations, review complaints, and exempt certain documents from freedom-of-information obligations. Under APP 13, individuals may request corrections to inaccurate or outdated personal information, requiring organisations to ensure the integrity and accuracy of collected data. Non-compliance may trigger investigations and remedial directives, including improvements to security measures and the imposition of fines. Recent reforms, reflected in the Privacy Amendment Bill 2024, mark a significant strengthening of Australia's data protection landscape. These reforms introduce measures such as the establishment of a Children's Online Privacy Code, updated cross-border transfer rules through a new whitelist mechanism, enhanced technical and organisational security obligations, and new criminal offences for doxing pertaining to the malicious publication of private information. The amendments also expand judicial powers to impose civil penalties, restitution orders, and compensation for victims of privacy breaches, reinforcing a culture of accountability and deterrence. Collectively, these developments signal Australia's shift toward a more robust and responsive privacy regime aligned with contemporary digital risks and international standards.

Complementing the Privacy Act are two sector-specific laws aimed at curbing unsolicited communications and reinforcing consumer control over personal data usage. The Spam Act 2003 regulates commercial electronic messages, prohibiting the sending of unsolicited emails, SMS, or instant messages without prior consent (Haydon & Wing, 2004). It also mandates the inclusion of accurate sender information and functional unsubscribe mechanisms. This Act is particularly relevant for e-commerce, where digital marketing is widespread, as it ensures that consumer data is not exploited for intrusive or deceptive communication practices. The Spam Act works in tandem with privacy principles by requiring organisations to obtain and document consent before engaging in electronic outreach (Holmes, 2003). Likewise, the Do Not Call Register Act 2006 establishes a national registry that enables individuals to opt out of receiving telemarketing calls. Organisations are legally required to check numbers against the register before initiating contact, thereby aligning marketing practices with consumer preferences. The DNC scheme reinforces broader privacy protections by preventing the misuse of contact information for unwelcome telemarketing and supporting informed choice in commercial communications (DiCecco, 2011). Together, the Spam Act and DNC Register Act extend Australia's data protection ecosystem beyond general privacy regulation, providing a holistic approach to the regulation of personal data in digital and telecommunications environments.

Methodology

This study adopts a doctrinal and comparative legal research methodology to examine the data protection frameworks applicable to e-commerce in Malaysia, Singapore, and Australia. Doctrinal research is appropriate because the inquiry is centred on analysing legal rules, statutory provisions, regulatory principles, and case law that govern the protection of personal data in commercial transactions (Hutchinson, 2013). Doctrinal research enables a systematic examination of primary legal sources to identify the current legal position, interpret statutory obligations, and understand the rights and responsibilities placed on organisations processing personal data (Gestel, 2023). The doctrinal component of the study

involves a detailed evaluation of primary legislation, including Malaysia's PDPA 2010, the Personal Data Protection Regulations 2013, the Data Protection Standards 2015, and related statutes such as the Consumer Protection Act 1999, Digital Signature Act 1997, and Computer Crimes Act 1997. For Singapore, the analysis focuses on the Personal Data Protection Act 2012, its subsequent amendments, and regulatory guidelines issued by the Personal Data Protection Commission (PDPC). In Australia, the study examines the Privacy Act 1988, the Australian Privacy Principles (APPs), and the Notifiable Data Breaches (NDB) scheme. Case law, including *Lew Cher Pow v Pua Yong Yong* in Malaysia and *Michael Reed v Alex Bellingham* in Singapore, is reviewed to shed light on judicial interpretation and the practical application of statutory provisions. The doctrinal analysis enables the study to identify the legal principles that structure each jurisdiction's approach to data protection, including consent requirements, purpose limitation, data security obligations, retention rules, and individuals' rights. This method further assists in identifying gaps, limitations, and areas of potential reform within the Malaysian framework.

To address the research questions concerning differences across the three jurisdictions, the study employs a comparative legal method. This comparative law methodology compares legal doctrines and rules based on the functions they serve within their respective legal systems (Cotterrell, 2017; Gordley, 2017). It involves the borrowing of legal ideas and institutions from one legal system to another(Bussani & Mattei, 2010). Comparative law provides insights that can inform legal reforms and the development of new legal frameworks. It helps identify best practices and innovative solutions from other jurisdictions (Sinani & Mehmeti, 2025). The paper compares main legislation on data protection, enforcement mechanisms, breach notification requirements, cross-border data transfer rules, organisational accountability, and consumer rights. This comparative approach is justified because Malaysia, Singapore, and Australia share a common law heritage yet demonstrate differing levels of regulatory maturity and institutional development. Comparing these jurisdictions allows for the identification of best practices and illuminates how particular regulatory choices may be adapted to the Malaysian context. The comparison also provides the basis for considering potential enhancements to Malaysia's PDPA 2010 in line with evolving technological and commercial realities.

Findings

This section presents the results of the doctrinal and comparative analysis by outlining the legal frameworks governing data protection in Malaysia, Singapore, and Australia and describing the key areas in which these frameworks differ. The findings draw directly from statutory sources, regulatory instruments, and comparative features highlighted in the Table 1.

Legal Frameworks Governing Data Protection in E-Commerce in Malaysia, Singapore and Australia

Malaysia regulates personal data in e-commerce primarily through the Personal Data Protection Act 2010 (PDPA 2010), which establishes seven core data protection principles applicable to commercial transactions(Ismail, 2012; Prasetyoningsih et al., 2024). The Act is supplemented by sectoral laws such as the Consumer Protection Act 1999, Digital Signature Act 1997, and Computer Crimes Act 1997, each supporting different aspects of online commerce including consumer rights, authentication, and cybersecurity. A significant recent

development is the introduction of Section 12B, which establishes a mandatory data breach notification regime. Under this new provision, data users must notify the Personal Data Protection Commissioner of any data breach within 72 hours of becoming aware of it and must inform affected individuals within seven days where the breach is likely to result in significant harm. This introduces a clearer accountability mechanism and aligns Malaysia more closely with international expectations for timely breach reporting. Nonetheless, the PDPA 2010 has been criticised for its narrow scope, particularly its exclusion of Federal and State Government bodies and several categories of data processing, raising concerns about the adequacy of protection in an increasingly complex digital environment (Alibeigi & Munir, 2020; Kamaruddin et al., 2025). Although the PDPA incorporates elements of the EU GDPR, it remains limited in key areas such as safeguards against automated decision-making and the strength of its enforcement mechanisms (Asbullah et al., 2021; Pour, 2025)

Singapore's framework is centred on the Personal Data Protection Act 2012 (Singapore PDPA), supplemented by the Do Not Call (DNC) Registry, sector-specific guidelines, and active regulatory oversight by the Personal Data Protection Commission (PDPC). The Act mandates organisational accountability, breach notification, and safeguards for sensitive data. Singapore adopts a broad application that includes digital marketing activities through the DNC regime. Australia's data protection regime is governed by the Privacy Act 1988, strengthened by subsequent amendments, including the Privacy Amendment Bill 2024. The Act applies to both public and private sectors, subject to thresholds for small businesses. Additional statutes such as the Spam Act 2003 and Do Not Call Register Act 2006 regulate unsolicited communications, thereby reinforcing consumer autonomy over personal data in e-commerce(Haydon & Wing, 2004). Australia's regulatory architecture is supported by the Office of the Australian Information Commissioner (OAIC), which exercises extensive investigatory and enforcement powers.

Comparative Overview of the Frameworks in Malaysia, Singapore and Australia

The comparative analysis reveals that Malaysia, Singapore, and Australia share several common foundations in their approach to data protection within e-commerce. All three jurisdictions recognise main data protection principles such as consent, purpose limitation, accuracy, data security, and obligations governing retention and disclosure(Kemp, 2022; Prasetyoningsih et al., 2024; Shahul Ikram, 2024; Sholehuddin et al., 2024). Each system also establishes a regulatory authority responsible for overseeing compliance, although the strength and independence of these bodies differ. These commonalities reflect a broader international trend towards safeguarding personal information in digital markets while supporting technological innovation and commercial development.

Despite these shared principles, significant differences emerge in the structure, enforcement capacity, and regulatory maturity of the three frameworks. Singapore and Australia demonstrate more comprehensive systems, especially in terms of enforcement mechanisms and organisational accountability. Both jurisdictions incorporate mandatory data breach notification requirements, ensuring that affected individuals and regulators are promptly informed of security incidents. Malaysia only recently introduced breach notification obligations through the insertion of Section 12B in the recent 2025 amendment to the PDPA 2010, representing a shift towards international best practices. Additionally, Singapore and Australia impose clearer obligations on organisations, such as Singapore's mandatory Data

Protection Officer requirement and Australia's detailed Australian Privacy Principles, which outline specific responsibilities across the data lifecycle. The comparison also shows notable variation in enforcement strength. Singapore's Personal Data Protection Commission (PDPC) and Australia's Office of the Australian Information Commissioner (OAIC) possess broader investigative and sanctioning powers compared with Malaysia's regulatory authority, which operates with more limited autonomy and lower penalties. This disparity contributes to differing levels of compliance culture among businesses in each jurisdiction. Furthermore, consumer rights are more developed in Singapore and Australia, where individuals benefit from clearer access, correction, and notification rights, and where proposals continue to push towards expanded protections such as data portability and enhanced transparency.

Cross-border data transfer regulation further distinguishes the three frameworks. Singapore and Australia adopt accountability-based models that allow transfers subject to contractual safeguards or comparable protection mechanisms. Malaysia's earlier whitelist system, now removed by the 2024 amendments, reflected a more restrictive and less flexible approach. The shift towards an accountability model indicates Malaysia's intent to align with more adaptable international practices, though practical implementation remains in early stages. Overall, the cross-jurisdictional findings illustrate that while Malaysia has established an important foundational framework through the PDPA, its regulatory maturity remains developing relative to Singapore and Australia. Both comparator jurisdictions provide models of stronger institutional oversight, clearer organisational duties, and more extensive consumer protections. These differences serve as a basis for later discussion on potential refinements that Malaysia may consider enhancing its data protection regime in the context of a rapidly expanding digital economy.

Main Divergences Across the Three Jurisdictions

This section highlights the main divergences of the legal framework on data protection in e-commerce in Malaysia, Singapore and Australia. Table 1 below highlighted the main differences across the three jurisdictions.

Table 1
Main Differences on the Data Protection Laws in E-Commerce in Malaysia, Singapore and Australia

Differences / Countries	Malaysia	Singapore	Australia
Methods of Enforcement and Penalties	• Personal Data Protection Act 2010 (Section 5(2))	• Personal Data Protection Act (PDPA) 2012 – amendments	• Privacy Act 1988 – 2024 amendments
Scope of Data Protection Laws	• PDPA applies only to commercial dealings (Section 4)	• PDPA; Do Not Call (DNC) Registry	• Privacy Act 1988 – applies to organisations with annual revenue exceeding AUD 3 million
Management of Sensitive Information	• Computer Crimes Act 1997 (Sections 3 & 6)	• PDPA (Section 15)	• Privacy Act (Section 6) • Privacy Amendment Bill 2024 – Children's Online Privacy Code
Cross-Border Regulation	• Malaysia's PDPA Amendment Bill 2024	• PDPA (Section 26)	• Spam Act 2003 (Section 16)

Methods of Enforcement and Penalties
Malaysia's enforcement is rooted in the PDPA 2010, with penalties historically more limited compared with the other jurisdictions. While recent amendments increase fines and introduce mandatory breach notification, enforcement capacity remains comparatively narrower than in Singapore and Australia. Singapore's PDPC issues binding directions and financial penalties, whereas Australia's OAIC may impose significant civil penalties and undertake broad compliance assessments. Australia's regime also incorporates new criminal offences such as doxing.

Scope of Data Protection Laws
Malaysia's PDPA applies solely to commercial transactions, excluding Federal and State Governments. This narrow scope contrasts with Singapore, where the PDPA covers private sector organisations broadly and complements the DNC Registry to regulate telemarketing practices. Australia's Privacy Act applies across sectors and includes organisations with annual turnover above AUD 3 million, creating a wider regulatory net.

Management of Sensitive Information
Malaysia's treatment of sensitive information is distributed across several statutes, including the Computer Crimes Act 1997. Singapore incorporates obligations under Section 15 of the PDPA to ensure reasonable security arrangements for personal data. Australia's Privacy Act provides a detailed definition of sensitive information and additional safeguards, with the 2024 amendments introducing a Children's Online Privacy Code to strengthen protections for minors.

Cross-Border Data Transfers

Malaysia's 2024 amendment replaces the earlier whitelist approach with an adequacy-based model, allowing transfers where comparable protection exists. Singapore requires that organisations ensure overseas recipients provide protection comparable to the PDPA, either through contractual clauses or PDPC-approved certifications. Australia applies cross-border rules under the APPs, holding organisations accountable for the acts of overseas recipients and supplementing this with sectoral laws such as the Spam Act 2003.

Discussion

The comparative analysis reveals several divergences between Malaysia, Singapore, and Australia, each with implications for the effectiveness, coherence, and future development of Malaysia's data protection framework. These divergences must be understood not only in terms of statutory design but also regulatory philosophy, enforcement culture, and institutional capacity. As Malaysia advances its digital economy agenda, reflecting on these differences provides valuable insights for strengthening its personal data governance.

Enforcement Capacity and Regulatory Culture

One of the clearest distinctions among the three jurisdictions lies in enforcement. Singapore and Australia maintain regulatory bodies which are the PDPC and OAIC, respectively and empower them with broad investigatory powers, the ability to issue binding directions, and authority to impose substantial financial penalties. These features contribute to a strong compliance culture and enable timely responses to data breaches and systemic risks (Soemitro et al., 2023). In contrast, Malaysia's enforcement framework remains comparatively modest. While the PDPA Amendment Bill 2024 introduces higher penalties and a mandatory breach notification mechanism (Section 12B), the overall enforcement model remains less robust, partly due to limited statutory powers and resource constraints. This divergence suggests that Malaysia may benefit from enhancing the autonomy and enforcement authority of the Personal Data Protection Commissioner, including clearer procedural powers for audits, investigations, and compliance assessments. A more empowered regulator could help ensure consistent compliance, deter violations, and support sector-specific guidance similar to the PDPC's advisory guidelines and OAIC's privacy practice directives.

Scope of Coverage and Consistency of Protection

Malaysia's PDPA applies exclusively to commercial transactions, excluding Federal and State public authorities. This creates gaps in protection and results in inconsistent standards across sectors. Singapore and Australia adopt broader and more integrated regulatory approaches, with Singapore's framework applying across the private sector, while Australia's regime extends to both public and private sectors, subject to statutory revenue thresholds (Yongquan, 2017). The exclusion of the Malaysian public sector from PDPA coverage is increasingly difficult to justify in an era where government agencies also process vast amounts of personal data, often in high-risk contexts such as health, welfare, and digital identity systems (Alibeigi & Munir, 2020). Extending the PDPA's scope or establishing parallel legislation for public-sector data processing would improve consistency, enhance public trust, and align Malaysia with international best practices. Such reforms would also reduce fragmentation and support cross-sectoral data governance, particularly in initiatives involving public–private data sharing.

Standards for Sensitive Data and Consumer Rights

Another area of divergence lies in the treatment of sensitive information. Australia's Privacy Act includes a detailed definition of sensitive information and imposes heightened protections, particularly with its introduction of the Children's Online Privacy Code (2024). Singapore similarly places strong emphasis on accountability and security arrangements, requiring organisations to take "reasonable measures" to protect sensitive data. Malaysia's PDPA historically featured a narrower conception of sensitive data; however, the 2024 amendments expand this to include biometric information and mandate stronger organisational obligations (Fauzi & Andriasari, 2025; Kemp, 2022). Nevertheless, Malaysia could further enhance its framework by developing more granular rules for specific categories of data, such as children's data, genetic data, and automated profiling. These refinements would strengthen the PDPA's responsiveness to contemporary digital risks, especially in e-commerce environments where behavioural profiling and targeted advertising are common.

Cross-Border Transfers and Global Data Flows

Cross-border data regulation is increasingly central to digital commerce. Singapore's PDPA and Australia's APPs impose accountability mechanisms on organisations transferring data abroad, requiring contractual safeguards, comparability assessments, or approved certification mechanisms (Kemp, 2022). Malaysia's shift from a whitelist to an adequacy-based approach is a positive step, yet its operational framework remains less defined. Clearer guidance on adequacy assessments, the use of standard contractual clauses, and binding corporate rules would improve certainty for businesses and strengthen Malaysia's position in regional digital trade ecosystems. Establishing a transparent, risk-based approach to cross-border transfers modelled on frameworks used in Singapore and Australia would help Malaysia better manage data flows associated with cloud services, regional e-commerce platforms, and multinational digital operations.

Potential Improvements for Malaysia

A review of Malaysia's existing Personal Data Protection Act 2010 (PDPA) and the comparative insights drawn from Singapore and Australia indicate several areas where Malaysia could enhance its data protection regime to better support e-commerce and align with global best practices. Although the PDPA provides a foundational framework, its limitations particularly in breach notification, data minimisation, enforcement, and governance suggest the need for targeted reforms to strengthen consumer trust and regulatory effectiveness. First, Malaysia could improve its framework by incorporating robust data limitation and minimisation principles. The literature stresses that organisations often collect excessive personal data, increasing exposure to breaches and misuse. Introducing explicit statutory obligations to limit collection, retain data only as long as necessary, and anonymise or pseudonymise data where possible would reduce systemic risks and align the PDPA with international norms such as the GDPR and Singapore's strengthened accountability model. Second, Malaysia should consider expanding its regulatory tools by enhancing governance and internal accountability mechanisms. In Singapore and Australia, data protection obligations are reinforced by strong organisational accountability requirements, including mandatory appointment of Data Protection Officers (DPOs) and documented internal policies. While Malaysia's recent amendments introduce DPO obligations, further strengthening of governance such as detailed breach-assessment duties, comprehensive record-keeping, and clearer procedural standards would promote organisational readiness and improve regulatory enforcement.

Third, cross-border data transfer rules could be made clearer and more flexible. The paper notes that Malaysia's amendments remove the former "white-list" system, enabling transfers to jurisdictions with comparable protection standards. However, Malaysia may still benefit from more detailed guidance on adequacy assessments, standard contractual clauses, and binding corporate rules to provide certainty for e-commerce operators engaged in regional or global data flows. Lastly, Malaysia should strengthen enforcement mechanisms and penalties. The recent increase in fines which is up to RM1 million or imprisonment for serious offences certainly marks significant progress, but effective enforcement requires sustained regulatory capacity, sector-specific oversight, and active compliance audits. Comparative jurisdictions, particularly Australia with its high penalties and proactive regulatory posture, demonstrate the importance of strong enforcement in shaping industry behaviour.

Taken together, these enhancements such as mandatory breach timelines, data minimisation standards, stronger governance duties, clearer cross-border transfer requirements, and reinforced enforcement structures offer a coherent roadmap for modernising Malaysia's data protection regime. By integrating these improvements, Malaysia can better support its expanding digital economy, cultivate consumer confidence, and align its regulatory environment with international best practices.

Conclusion and Recommendations

The rapid expansion of e-commerce in Malaysia, Singapore, and Australia has amplified the need for a stronger personal data protection framework capable of regulating increasingly complex digital ecosystems. This study set out to answer three central questions: (i) the laws governing data protection in e-commerce in the three jurisdictions, (ii) the ways in which these frameworks differ, and (iii) the improvements Malaysia could consider as its regulatory landscape evolves. The doctrinal and comparative analysis demonstrates that while Malaysia's PDPA 2010 provides an essential foundation for data governance, it remains less comprehensive and less institutionally developed compared with Singapore's mature accountability regime and Australia's sophisticated enforcement architecture. Malaysia's recent reforms, particularly the introduction of mandatory breach notification under Section 12B, the shift to an adequacy-style cross-border transfer model, and improvements in organisational accountability mark meaningful progress. These developments reflect an increasing alignment with international norms and a recognition of the risks posed by online transactions, cyber incidents, and cross-border data flows. Nonetheless, the research reveals continuing structural gaps, including the PDPA 2010's narrow scope, the absence of robust minimisation and automated decision-making safeguards, limited enforcement powers, and insufficiently detailed guidance on governance obligations. These gaps contrast sharply with Singapore's clear DPO requirements, detailed advisory guidelines, strong PDPC enforcement culture, and Australia's expanding APP-based obligations, high penalties, and specialised protections such as the Children's Online Privacy Code and sector-specific anti-spam and telemarketing regulations. Overall, the findings indicate that Malaysia stands at a critical juncture. As e-commerce becomes increasingly data-intensive, Malaysia must move towards a more coherent, rights-centred, and enforcement-driven regime if it is to sustain public trust, support digital trade, and align with global privacy expectations.

The paper proposes several recommendations to enhance Malaysia's data protection laws in light of comparative insights from Singapore and Australia:

Strengthen the Scope and Enforcement of the PDPA

Extend the PDPA to cover public-sector data processing, enhance the investigative and sanctioning powers of the Personal Data Protection Commissioner and introduce administrative penalties to promote stronger regulatory compliance.

Enhance Organisational Accountability and Governance Obligations

Require clearer governance measures such as mandatory Data Protection Officers, internal privacy management programmes, data-retention policies and regular compliance audits to cultivate a proactive privacy culture among organisations.

Introduce Stronger Substantive Protections for Individuals

Incorporate explicit statutory requirements on data minimisation, purpose limitation, and safeguards against automated decision-making and profiling, alongside expanded protection for sensitive categories of data including biometric and children's information.

Improve Cross-Border Transfer Mechanisms and Sector-Specific Guidance

Provide detailed operational tools-such as standard contractual clauses, binding corporate rules, and adequacy criteria-to guide international data transfers and introduce sector-specific guidelines for high-risk areas such as e-commerce platforms and digital marketplaces.

References

Alibeigi, A., & Munir, A. B. (2020). Malaysian personal data protection act, a mysterious application. *University of Bologna Law Review*, *5*(2), 362–374. https://doi.org/10.6092/ISSN.2531-6133/12441

Alibeigi, A., Munir, A. B., & Asemi, A. (2021). Compliance with Malaysian Personal Data Protection Act 2010 by banking and financial institutions, a legal survey on privacy policies. *International Review of Law Computers and Technology*, *35*(3), 365–394. https://doi.org/10.1080/13600869.2021.1970936

Aryani, D. N., Nair, R. K., Hoo, D. X. Y., Kee, D. M. H., Lim, D. H. R., Chandran, D. A. P. R., Chew, W. P., & Desai, A. (2021). A study on consumer behaviour: Transition from traditional shopping to online shopping during the COVID-19 pandemic. *International Journal of Applied Business and International Management*, *6*(2), 81–95. https://doi.org/10.32535/ijabim.v6i2.1170

Asbullah, S., Mohamad, M. D., Abdullah, S. F. S., & Shahruddin, M. S. (2021). Strengthening mediation in neighbourhood dispute: An Islamic input. *Environment-Behaviour Proceedings Journal*, *6*(SI5), 19–24. https://doi.org/10.21834/ebpj.v6isi5.2924

Begum, V. V., & Kavitha, M. (2023). Blockchain technology in the marketing sphere. In *Blockchain the Chain for the Changing Marketing Sphere*.

Bussani, M., & Mattei, U. (2010). The Cambridge companion to comparative law. In *Cambridge Companion to Comparative Law*. https://doi.org/10.1017/CBO9781139017206

Channak, Z. M., Alkhateeb, A., Saleh, E., Aldeeb, H., & Alsharif, S. (2023). Business ethics in E-commerce – legal challenges and opportunities. *Access to Justice in Eastern Europe*, *6*(Special Is), 1–16. https://doi.org/10.33327/AJEE-18-6S007

Cotterrell, R. (2017). The concept of legal culture. In *Comparing Legal Cultures*. https://doi.org/10.4324/9781315259741-9

DiCecco, V. (2011). Play by the rules. *Printwear*, *24*(9), 28–31.

Fauzi, M. F., & Andriasari, D. (2025). Studi perbandingan hukum pidana perlindungan data pribadi di Indonesia dan Singapura. *Bandung Conference Series Law Studies*, *5*(2). https://doi.org/10.29313/bcsls.v5i2.19214

Gestel, R. van. (2023). Quality, methodology, and politics in doctrinal legal scholarship. *Law and Method*. https://doi.org/10.5553/rem/.000070

Goh, L. (2018). Can Singapore learn from the European Union in tightening data protection laws? *Journal of Data Protection & Privacy*, *1*(4), 384. https://doi.org/10.69554/tpqq5783

Gordley, J. (2017). Comparison, law, and culture: A response to Pierre Legrand. *American Journal of Comparative Law*, *65*, 133–180. https://doi.org/10.1093/ajcl/avx017

Haydon, J., & Wing, A. (2004). Stopping spam - The way forward. *Telecommunications Journal of Australia*, *54*(1), 47–67.

Holmes, J. (2003). Spam - Relief at last. *Telecommunications Journal of Australia*, *53*(4), 33.

Hutchinson, T. C. (2013). Doctrinal research : Researching the Jury. In D. Watkins & M. Burton (Eds.), *Research Methods in Law* (pp. 7–33). Routledge (Taylor & Francis Group).

Ismail, N. (2012). Selected issues regarding the Malaysian Personal Data Protection Act (PDPA) 2010. *International Data Privacy Law*, *2*(2), 105–112. https://doi.org/10.1093/idpl/ips005

Kamaruddin, S., Abdikhakimov, I., Hamin, Z., & Saufi, N. N. M. (2025). The conundrum of personal data protection in Malaysia. *Journal of Data Protection and Privacy*, *8*(1), 65–77. https://doi.org/10.69554/GPYM2949

Kamila, A. L., Budiono, A., & Ikrima, N. A. (2025). Legal policy for name impersonation victims in online loans: A comparison between Indonesia and Singapore. *Audito Comparative Law Journal (Aclj)*, *6*(3), 175–186. https://doi.org/10.22219/aclj.v6i3.40969

Kemp, K. (2022). Strengthening enforcement and redress under the Australian Privacy Act. *Global Privacy Law Review*, *3*(3), 150–162. https://doi.org/10.54648/gplr2022016

Kennedy, G., Wong, J., Babu, A., Poti, G., Taher, A. Y., Nakaoka, K., Chia, J., Yew, B., Ngan, K., Nian, L. C., Lee, H., & Vu, Q. M. (2025). Asia–Pacific developments. *Computer Law & Security Review*, *57*, 106151. https://doi.org/10.1016/J.CLSR.2025.106151

Kiu, C.-C., & Lee, C.-S. (2017). E-commerce market trends: A case study in leveraging Web 2.0 technologies to gain and improve competitive advantage. *International Journal of Business Information Systems*, *25*(3), 373–392. https://doi.org/10.1504/IJBIS.2017.10005086

Mannan, M. A. (2024). Data privacy in e-commerce: Challenges and best practices. In *Analyzing Privacy and Security Difficulties in Social Media New Challenges and Solutions*. https://doi.org/10.4018/979-8-3693-9491-5.ch017

Marx, M. J. L. a. k. a, & Niasin, M. A. F. (2023). Diffusion of innovation of e-commerce among service sector SMEs in Malaysia during and post-pandemic Covid-19: A qualitative approach. *Environment-Behaviour Proceedings Journal*, *8*(SI15), 31–36. https://doi.org/10.21834/e-bpj.v8isi15.5073

Mohamad, A., Angsor, M. A. M., Adi, M. N. M., & Min, A. T. J. (2025). *Malaysia's e-commerce landscape: Legal structures and operational hurdles*. 45. https://doi.org/10.1117/12.3059023

Mohamad, Z., Ismail, Z., & Thani, A. K. A. (2023). Determinants of fraud victimizations in Malaysian e commerce: A conceptual paper. *International Journal of Academic Research in Business and Social Sciences*, *13*(12). https://doi.org/10.6007/ijarbss/v13-i12/20395

Nadzri, W. N. M., Hashim, A. J. C., Majid, M., Jalil, N. A. A., Alzoubi, H. M., & Alshurideh, M. T. (2023). Share your beautiful journey: Investigating user generated content (UGC) and webrooming among Malaysian online shoppers. In *Studies in Computational Intelligence* (Vol. 1056). https://doi.org/10.1007/978-3-031-12382-5_124

Narayanasamy, K., Jacobs, C. J. G. M. C. N., & Seyapalan, P. S. D. (2017). Legislating consumer law in Malaysia and the consumers' apprehension. *International Journal of Economic Research*, *14*(15), 135–150.

Noor, A. A. bin M., Haron, N. H., Rohani, S. R. S., & Rahman, R. binti A. (2022). Covid-19 Pandemic and online fraud: Malaysian experience. *International Journal of Academic Research in Accounting Finance and Management Sciences*, *12*(4). https://doi.org/10.6007/ijarafms/v12-i4/14172

Patro, S. P., Padhy, N., & Panigrahi, R. (2016). Security issues over e-commerce and their solutions. *Ijarcce*, *5*(12), 81–85. https://doi.org/10.17148/ijarcce.2016.51216

Pour, H. N. (2025). Data protection challenges in smart cities: an examination of the Malaysian legal framework. *Uum Journal of Legal Studies*, *16*(1), 115–129. https://doi.org/10.32890/uumjls2025.16.1.7

Prasetyoningsih, N., Ismail Nawang, N., Putri, W. V., & Amirullah, M. N. R. (2024). Legal protection for the personal data in indonesia and Malaysia. In *Lecture Notes in Computer Science Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics: Vol. 14728 LNCS*. https://doi.org/10.1007/978-3-031-61379-1_11

Pregoner, J. D., Opalla, I. L., Uy, J. D., & Palacio, M. (2020). *Customers' perception on the trustworthiness of electronic commerce: A qualitative study*. https://doi.org/10.35542/osf.io/msdpg

Raghavan, A., Demircioğlu, M. A., & Taeihagh, A. (2021). Public health innovation through cloud adoption: A comparative analysis of drivers and barriers in Japan, South Korea, and Singapore. *International Journal of Environmental Research and Public Health*, *18*(1), 334. https://doi.org/10.3390/ijerph18010334

Rajkumar, K. V., Yadav, O. V., Bhyrapuneni, S., Sudha, M. V., Ratnagiri, D., & Thota, K. K. (2024). Enhancing e-commerce security: A machine learning framework for fraud detection. *8th International Conference on Electronics Communication and Aerospace Technology ICECA 2024 Proceedings*, 942–947. https://doi.org/10.1109/ICECA63461.2024.10801104

Razali, N. A. H., Rosli, W. R. W., & Othman, M. B. (2022). The legal protection of e-consumers against e-commerce fraud in Malaysia. *Malaysian Journal of Social Sciences and Humanities*, *7*(9), e001778. https://doi.org/10.47405/mjssh.v7i9.1778

Seah, C. S., Loh, Y. X., Wong, Y. S., Jalaludin, F. W., & Loh, L. H. (2022). The Influence of COVID-19 pandemic on Malaysian e-commerce landscape: The case of Shopee and Lazada. *ACM International Conference Proceeding Series*, 215–221. https://doi.org/10.1145/3537693.3537726

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

Sholehuddin, N., Miskam, S., Shahwahid, F. M., Aziz, T. N. R. A., & Mansor, N. (2024). A comparative legal analysis on personal data protection laws in selected ASEAN countries. *Journal of Muwafaqat*, *7*(1), 23–38. https://doi.org/10.53840/muwafaqat.v7i1.166

Sinani, B., & Mehmeti, S. (2025). The importance of comparative law for the development of contemporary law. *Juridical Tribune Review of Comparative and International Law*, *15*(1), 5–23. https://doi.org/10.62768/TBJ/2025/15/1/01

Sirurmath, S. S., & Pani, A. K. (2004). E-commerce strategies for library and information services. *Digital Information Exchange Pathways to Build Global Information Society*, 536–542.

Soemitro, D. P., Wicaksono, M. A., & Putri, N. A. (2023). Penal provisions in the personal data protection law: A comparative legal study between Indonesia and Singapore. *Sign Jurnal Hukum*, *5*(1), 155–167. https://doi.org/10.37276/sjh.v5i1.272

Udayaprasad, P. K., Shreyas, J., Flammini, F., & Lin, H. (2025). Cyber security issues, Challenges in e-shopping/e-commerce. In *Cyber Security in Business Analytics*. https://doi.org/10.1201/9781003540045-3

Waters, N. (2012). Responding to new challenges to privacy through law reform: A privacy advocate's perspective. In *Emerging Challenges in Privacy Law Comparative Perspectives*. https://doi.org/10.1017/CBO9781107300491.005

Yeon, A. L., Yaacob, N., Hussain, M. A., & Ismail, C. T. M. (2022). Equity crowdfunding vs cybercrime: A legal protection. *Bild Law Journal*, *7*(1), 139–150.

Yongquan, B. W. (2017). Data privacy law in Singapore: The Personal Data Protection Act 2012. *International Data Privacy Law*, *7*(4), 287–302. https://doi.org/10.1093/idpl/ipx016

Zulham. (2023). A critical review of consumer protection online shopping, false advertising and legal protection. *Journal of Law and Sustainable Development*, *11*(5). https://doi.org/10.55908/sdgs.v11i5.740