Asian Journal of Law and Policy
Vol. 6 No. 1 (March 2026) eISSN: 2785-8979

Safeguarding Consumers' Privacy in Malaysia's Digital Economy Landscape

Jing Xie Lim
Faculty of Law, Universiti Tekonologi MARA, Malaysia
limjingxie@uitm.edu.my
ORCID iD: 0009-0006-9399-3380
(Corresponding author)

Farah Adibah Zulkifli
Faculty of Law, Universiti Tekonologi MARA, Malaysia
farahadibah@uitm.edu.my
ORCID iD: 0009-0007-6967-2568

ABSTRACT

This study aims to explore the extent of application of the Personal Data Protection Act 2010 (PDPA) in Malaysia with regard to protecting privacy and avoiding the misuse of personal data when it comes to consumers buying from businesses operating through online platforms. It intends to determine the challenges faced by e-commerce platforms in ensuring the protection of private data from cyber-attacks and cyber troops and the issue of regulating cross-border data flows. This study also compares the PDPA with the European Union's General Data Protection Regulation (GDPR) and Australia's Privacy Act 1988 to identify improvements to the PDPA to make it more comprehensive and cater to the e-commerce industry. The study reveals that the PDPA provides protection for consumers buying from online platform businesses. However, there is a need for proactive cybersecurity measures by the online platforms operators to ensure the private data of the consumers are protected from cyber-attacks. Cross-border data flow is also a concern due to the lack of rules between nations on the mechanism to regulate data across borders. The EU's GDPR is a possible solution, which also strengthens data protection and business opportunities in the digital market which is lacking in the PDPA. It would also be beneficial for Malaysia to look into Australia's Privacy Act 1988 as a benchmark for how non-EU state legislation adapts to the GDPR. These reforms ensure alignment with the SDG goals.

(2026) Asian Journal of Law and Policy, 6(1), 1–21
https://doi.org/10.33093/ajlp.2026.1
© Universiti Telekom Sdn Bhd. This work is licensed under the Creative Commons BY-NC-ND 4.0 International License.
Published by MMU Press. URL: https://journals.mmupress.com/ajlp

Keywords: Digital economy; Consumer rights; General Data Protection Regulation; Privacy; Personal Data Protection Act 2010; Sustainable Development Goals

Received: 9 April 2025, **Accepted:** 20 June 2025, **Published:** 31 March 2026

1. Introduction

Our daily activities are intertwined with digitalization. Anywhere you go, you see people scrolling and scrolling on their smartphones, be it on social media or playing music. The Internet and social media have become integral parts of our lives. According to the Internet Users Survey 2022 published by Malaysian Communications and Multimedia Commission (2024). It was indicated that the percentage of Internet users in 2022 was estimated at 92.7%, which shows an increase of 4.0% from 88.7% compared to the year 2020. This shows that people are spending more time on the Internet. Thus, social media has been a major mechanism for businesses to reach out and connect with their customers. It has become a bridge that links consumers and products. Anything can easily go viral on social media, such as Facebook and TikTok, within seconds, as most people would read and watch reviews about products before purchasing. This shows that most people are influenced by information they see on social media (Darmatama & Erdiansyah, 2021), which also causes a huge spike in the digital economy, especially since COVID-19, where online shopping has become the norm in our lives. However, this also exposes consumers to various challenges and threats as they are considered to be vulnerable in this environment. For people to gain access to these products, they have to download many applications on their smartphones, sign up for accounts which eventually expose their personal data online.

Globalisation of the digital economy, such as online shops and online sales are depriving consumers of their rights to be able to inspect and check for goods during or before a sale. Online platforms allow consumers to purchase products and services online at the tips of their fingers. They are able to search for and select their products of interest from various retailers on the website. The rise of Malaysia's digital economy aligns with sustainable development goal (SDG) 9, which is industry, innovation, and infrastructure. This brings technological progress to the country. While this brings convenience to consumers, this also exposes consumers' personal data, especially when they accept terms of a public offer, some resulting in unauthorised collection of personal data of customers by the business. Safeguarding customer data in online transactions is essential for achieving SDG 16, which is peace, justice, and strong institutions when it comes to responsible data governance. The e-commerce industry relies on Big Data to personalise advertisements for consumers, which is a popular marketing strategy. This sparks concerns about privacy and misuse of personal data, such as data profiling, which enables the platform to 'predict' what a consumer prefers. In Malaysia, personal data protection falls under the Personal Data Protection Act (PDPA), which came into force and was gazetted in 2013. However, the PDPA does not have any special provisions that specifically addresses the issue of privacy online, especially on social media where business entities are making online shopping more and more common, especially during the COVID-19 pandemic era, when people tend to go out

less and go online more often. The new legislation, namely the Data Sharing Act 2025 (Act 864) which received royal assent recently, although yet to come into force, establishes support for development of artificial intelligence (AI) and facilitates data exchange between public sectors, which also supports consumer privacy indirectly through its strict evolution on data sharing and its confidentiality.

2. Research Problem

Data privacy and trust are major challenges for online businesses. In order to make purchases on an online shopping platform, consumers are required to provide private data such as their name, email address, a unique password, date of birth, address, and etc. Some websites also require a bank account number for the purpose of the auto debit process. These data are relatively important and significant for the consumer as a data subject, as it will cause infringement of privacy to the owner of these data if it were being misused which is in accordance with the Personal Data Protection Act (PDPA) 2010. Although online shopping platforms often state the purpose of the collected data and its usage within the website, such as for research and analysis purposes, the questions that arise here are how this research and analysis are being done, which data are involved, who is the person processing it, and which parties are involved. Most online shopping privacy does state that the data might be shared to the third party for the purpose of providing the customer with a better service but there is no clear guidance as to how these processes should be done (Bin Noor Azman & Awang, 2020).

Online shopping also exposes consumers to possible private data infringement when their shopping histories can be tracked and analysed by the online platforms for the purpose of market research, personalised and targeted marketing and other forms of clients' manipulations. These online platforms may also sell their collected data about their clients to third parties (Groppe et al., 2018). However, it has been argued that this does not fall under the intrusion of privacy. It was concluded that predictive analytics over the personal data is not protected under PDPA as the data used during the process of analysis will not determine any specific individuals as defined under the PDPA 2010 (San, 2020). It was further argued that predicting an individual behaviour in a similar group of people as shown in the above example can cannot be said to cause any privacy intrusion or harm to a person's privacy. If the law imposed the unlimited right to the data subject over predictive analytics activities, this would open a floodgate to claims of privacy invasion (San, 2020).

In consideration to the global nature of commerce and people's movements, the European Union introduced the General Data Protection Regulation (GDPR) which represents the most significant data protection and privacy regulation replacing the outdated 1995 Data Protection Directive. One of the unique features of the GDPR is it covers any organisation that collects or processes EU citizen data independent of the data which was processed outside the EU unlike our PDPA which does not apply to personal data processed outside Malaysia.

Hence, this paper intends to discuss the followings:

(1) How does the Personal Data Protection Act (PDPA) in Malaysia apply to business organisations in the process of collection, storage, and utilisation of user data by businesses operating online.

(2) The primary challenge faced by e-commerce in complying with the PDPA and at the same time analyse data collected for marketing strategies.

(3) The comparison between the mechanisms used by the GDPR and PDPA to ensure data protection for consumers on online shopping platforms and whether GDPR principles can be considered by the policymakers in an effort to enhance data protection for consumers in Malaysia.

3. Research Methodology

This study employed doctrinal legal research to evaluate the ways the Malaysian Personal Data Protection Act (PDPA) applies to business organisations operating online, the primary challenges faced by e-commerce in complying with the PDPA as well as the comparison between the mechanism used by the European Union's General Data Protection Regulation (GDPR), Malaysia's PDPA and the Australia's Privacy Act 1988 in ensuring data protection for consumers on online shopping platforms. Doctrinal legal research involves 'analysis of case law, arranging, ordering and systematising legal propositions and the study of legal institution through legal reasoning or rational deduction.' Both primary and secondary sources of law were examined through online database resources such as Lexis Legal Research for Academics, Springerlink, Elsevier, as well as websites of relevant legal institutions. The primary sources of law such as statutes, rules, regulations and other regulatory instruments was rigorously analysed. It is also supported by secondary sources of law including textbooks, journal articles, seminar papers, newspaper articles, online websites and other periodicals.

In addition, a comparative law method was used to achieve the objective of this study. Comparative law is the act of comparing the law of one country with another country It which not only furnishes information about the various laws from other countries for the legal issue in question, but also may provide solutions for many problems, or may help to avoid possible problems. They can make one aware of the fact that there is much to learn from the experiences of other legal systems or legal cultures. With a view to propose recommendations to enhance data protection for consumers in Malaysia, two jurisdictions have been chosen namely the European Union and Australia. The reason for choosing the EU's GDPR is due to the fact that the GDPR has a broad, extraterritorial scope, which applies to any entity processing data of European Union residents, regardless of the entity's location and is said to be the world's most comprehensive data privacy law. On the other hand, Australia's Privacy Act 1988 was reformed in 2014 and 2018 in order to keep up with current technology and extend its protections in accordance with the GDPR. Hence, it would be beneficial to compare between the Privacy Act 1988 and the PDPA to explore through

Australia's experience on adopting the GDPR into our own legislation. Thus, a comparative law study with these countries seems to be indispensable. The strengths and weaknesses of both GDPR and the Privacy Act 1988 were analysed and recommendations were made based on the approaches considered as the most viable with the existing legislations we have in Malaysia.

4. Understanding Digital Economy in Malaysia

Digitalization affected trade, service providers and social services including medicine and education (Polyakov & Kovshun, 2021). This causes business entities and consumers to rely on the Internet and the World Wide Web for businesses (Ramaiah, 2019). Most, if not all companies have adopted and incorporated digital technology in running their businesses. These enterprises are involved in the digital economy, which has become a substitute to traditional sale and purchase technology. It refers to the online activities involving the economy among people, business entities, electronic devices, and the data on the Internet. To simplify, it is an economic activity that provides products and services online via the Internet (Kosimov & Ruziboyeva, 2022). The convenience of the Internet has been the main source and reference for business structure, from how businesses interact to consumer behaviour. This creates the need for digital currency, where you transfer currency via transactions online. For example, in Malaysia, consumers and businesses have been using e-wallets since 2019, like Grab, Boost and the Touch 'n Go e-wallet (Bakar et al., 2020, p. 10). All these digital payment systems open the pathway to international business opportunities, where it allows flow of currency as long as there is Internet (Beh, 2019, p. 3).

As 4G and 5G networks become increasingly accessible, digital payment has also become more advanced. However, this also raises concern about privacy and consumer information being misused by unauthorised third parties (Yuvaraj & Sheila Eveline, 2018). This is because technological improvement also increases the level of risk consumers face. Smartphones and the Internet have certainly made online shopping accessible anytime anywhere. As the digital economy relies heavily on data and communication technology, it is only common when certain consumers start to worry about the safety of online shopping. This includes disseminating information people post on their social media accounts. With so much information and data published online, merchants and businesses realise that they could use information read and collected to reach and engage with certain groups who might be interested in their merchandise. Smart devices users usually do not have control over the information and data provided, as it is usually the devices 'sharing' information with each other on the Internet (Hsu & Lin, 2016). This raise concerns on how much information could a stranger have of a person just from social media, although no one should be naïve enough to believe that their content on any social media platform is fully confidential. It has been known that social media, like Facebook, allows commercial companies who does advertising to address and reach out to groups of people online via data profiling. This profiling raises concerns about the information that social media companies gather about their users and the application they make about this information

(Segado-Boj & Díaz-Campo, 2020). This raises several issues such as privacy and human rights, data protection and public interest. The right to an individual's privacy is a new and strange terminology in Malaysia. On 15 November 2013, the Personal Data Protection Act 2010 (PDPA) came into force in Malaysia. The Act, which oversees the processing of personal data of individuals involved in commercial transactions and prevents misuse or abuse of data in any kind.

As people and businesses rely more and more on social media, many businesses have turned to digital advertising. It is an effective marketing strategy to attract and influence consumers and create major branding effects (Foerster-Metz et al., 2018). They use Big Data and Analytics to discover patterns, correlation, consumer preference and market trends to collect useful information (Robinson et al., 2023). This creates a need for strong data security. All businesses should be able to ensure a superb level of security when it comes to collecting and storing individual data collected from consumers from business transactions. Article 8 of the EU Charter of Fundamental Rights emphasizes protection of personal data as a fundamental right which is especially essential in this digitalized society. However, there seemed to be quite a vague concept on whether it could be used on private parties and businesses. There are concerns on whether these data could cause infringement on an individual's privacy. The PDPA in Malaysia protects information collected on commercial transactions but is silent on data collected on social media run by businesses. Data are valuable assets to an organisation, as well as to individuals. The issue is whether businesses can use and analyse these data for their business strategies.

5. The Regulatory Framework in Malaysia: The PDPA

The right to privacy online is recognized in Malaysia under the right to life under Article 5(1) of the Federal Constitution. As the term 'personal liberty' encompasses a wide range of values connected with rights and freedom of an individual, it is only sensible and relevant to include the protection of the right to privacy under the scope and coverage of personal liberty. A constitutional right to privacy has the potential to fill up the gaps in the current legal practice when it comes to the right to privacy on social media in Malaysia. From the interpretation and decision of recent court cases regarding the right to privacy, it could be summarised that the courts do recognise that there is a right to privacy under the right to life. The law in Malaysia does recognise and will appropriately protect a right of personal privacy, although it does not cover when an individual invades the privacy of another private individual.

Generally, the right to privacy is recognized under several legislations in Malaysia, although not expressly provided. Apart from the constitutional protection under Article 5 of the Federal Constitution and common law principles, which were indirectly applicable. The right to privacy online is recognized in Malaysia under the right to life under Article 5(1) of the Federal Constitution. As the term 'personal liberty' encompasses a wide range of values connected with rights and freedom of an individual, it is only sensible and relevant to include the protection of the right to privacy under the scope and coverage of personal

liberty. A constitutional right to privacy has the potential to fill the gaps in the current legal practice regarding the right to privacy on social media in Malaysia. The legislation in Malaysia that directly deals with an aspect of privacy interest, which is data privacy, is the PDPA. It aims to protect an individual's personal data. As information on social media is also data, the PDPA is applicable to prevent invasion of privacy on social media, especially when commercial transactions are concerned. The PDPA safeguards and protects privacy and enables certain authorised information analysis. 'Personal data' was defined as any information in commercial transactions, which means that it is only applicable to personal data with commercial connections. Social media has become a platform for businesses, where they collect and process data via Big Data. Under Section 6 of the PDPA, the platform requires data users to get consent from the data subjects (consumers and users) before processing them for any purpose. The terms of consent was not defined, but section 3(1) of the PDPA mentions that consent could be obtained in 'any form', thus impliedly saying that consent could be also orally given, as long as it could be properly recorded and maintained by the data users (Sidi Ahmed & Zulhuda, 2019). However, it must be noted that the PDPA does not apply to the Federal and State government, non-commercial transactions, personal and private matters and data processed outside Malaysia's jurisdiction.

In Malaysia, data users based in Malaysia must comply with the seven PDPA rules, namely:

General Principle

Data users must obtain written consent from the data subject prior to any processing of personal data directly related to their website activities, necessary for legal purposes and limited to the minimum requirements only.

Notice and Choice Principle

The data subjects must be informed that the website they are accessing will be collecting certain information for processing and analysing in the future. Each website based in and running their businesses in Malaysia must have a policy statement written in both English and Malay informing the data subject their intent to collect data, what kind of data for which purposes, whether it shall be shared, rights of data subject and the organisations' contact information. All these are usually done via a Privacy Policy statement which is shown to the users when they visit the said websites.

Disclosure Principle

Data users are not allowed to share nor disclose a data subject's personal data, unless prior consent has been obtained (agreement to private policy). Information and personal data are protected from unauthorised third parties agreed upon by the data subject. The data collected can only be used for the purpose specified in the privacy policy disclosed to the data subject.

Security Principle

Under Section 9, it is stated that businesses should take necessary precautions to safeguard personal data, and at the same time ensure they comply with the measures undertaken.

Retention Principle

Under section 10(1) and 10(2), the data collected shall only be kept for the time required. The data user is responsible for taking reasonable steps for erasing and discarding said information. However, the PDPA is silent on the ideal period of retention of data.

Data Integrity Principle

Section 11 emphasises the importance of data integrity by highlighting how it is dependent on many factors like accuracy, completeness and the up-to-dateness of the data. It stresses that data users should evaluate reliability, source, and purpose to determine reasonableness.

Access Principle

The data use must give access to data subjects when data becomes outdated. This is because Section 12 provides that outdated data can be corrected and rectified. Data subjects have the right of access to personal data.

In Malaysia, there is also a Personal Data Protection Commissioner (PDPC) who serves as the authority for data protection, overseeing the processing of personal data in commercial transactions to prevent misuse of data. Non-compliance of the PDPA is punishable with criminal liability. To meet these legal requirements, many business organisations have designed their own privacy policies which requires users and consumers to agree to the terms before proceeding with any service they provide. They are required under the law to inform individuals on the data being processed, type data to be collected, purpose of processing, third parties to whom the data user may disclose the personal data and whether it is obligatory or voluntary for the data subject to supply the personal data. They are also not allowed to disclose personal data to a third party without consent from the subject data. It is also the responsibility of the organisations to take the necessary steps and precautions to protect these data, and to make sure these data are destroyed permanently when the purpose of processing these data is no longer needed. Privacy policies play an integral role to inform customers about their privacy online. However, according to a study carried out in 2017 (Chua et al., 2017), the compliance level of companies to the PDPA is low, which is a great concern and could affect consumers' trust towards organisations.

Another important part of privacy online in Malaysia are privacy policies provided by websites and shopping platforms. Policies online could affect consumer behaviours (Xian et al., 2023). Online shopping platforms like Shopee empowers its users by asking for consent before collecting data for marketing purposes. This gives data subjects the choice on whether

to have their information processed or not. Shopee sends notifications to users requesting permission before beginning data collection. By actively and asking multiple times, customers are well informed and are aware of the data collection process. Besides, Shopee also works hard in maintaining confidentiality of consumer information, implementing a mixture of measures for security of customer's data. They also took the necessary steps to ensure that their privacy policy adhered to the legal framework of the PDPA in Malaysia. They also provide clear information on the data collection process and how the platform intends to use these data. As privacy is a crucial factor in consumer behaviour, Shopee's efforts to comply with laws and provide adequate consumer behaviour can influence the overall attitude and subsequent shopping behaviours of the customers.

In Malaysia, the PDPA is the main regulation governing the handling of personal data in commercial transactions. The seven principles outlined in the PDPA must be followed by merchants. Online shopping platforms like Shopee should always ensure they comply with any new updates to maintain consumer confidence.

In addition to the PDPA, the new Data Sharing Act 2025 shows a significant move by Malaysia to facilitate and regulate data sharing among public sector agencies, creating a structured framework for more secure and responsible data sharing. There guidelines in the new act is complementary to balance the need for data-driven innovation in Malaysia's digital economy with the basic rights to consumer privacy. This reduces the ambiguity in cross-border data regulations. Both the PDPA and Data Sharing Act 2025 complements each other in promoting and creating a safer and more efficient e-commerce society for consumers.

6. Challenges and Concerns

Privacy is a unique concept, has a wide and Invasion of privacy is not a tort under the common law.[1] The emergence of Big Data has created a lot of business opportunities to improve their decision-making plans through the analysis of the data obtained online. Big Data is able to identify and discover a pattern of a person's activities on social media, be it a search for a person or something the user is interested in. This is because many people tend to share their personal interests and life on social media, especially influencers who have millions of followers.

With the emergence and evolution of the Internet of Things (IOT), the relationship between Big Data and individual privacy are further tangled. When Internet users surf the Internet or download new applications on their smart devices, most allow synchronisation among accounts, increasing the risk and chances of more data being collected and stored online (Adams, 2017). Internet users become more vulnerable to cyber-attacks, which lead to data breaches. It could cause significant financial losses to the victims and also harm to their social reputation. It could also cause identity theft and threaten national security.

[1] *Malone v. Metropolitan Police Commissioner* [1979] Chancery Division 344.

There is need for proactive cybersecurity measures by the organisations operating online platforms and applications as these online websites have become targets for cyber-troops aiming to cause chaos by disrupting essential services (Green, 2022). Society should also be educated and be more alert about the risks and rights to privacy online. Training and education programs can help the people to understand the risks they face online.

Individuals, businesses and the government should cooperate to come up with comprehensive and effective efforts for data subjects. Organisations should research and strengthen their cybersecurity system. They should be able to detect abnormalities and respond to cyber-attacks in real-time, providing a safer and more resilient environment in the digital age.

Another concern regarding privacy when it comes to e-commerce is cross-border data flows. As the Internet is a global network of computers, each user has their own unique Internet Protocol (IP) address, data and information are broken into little 'packets' before being transmitted. Cross-border data transfers allow consumers to access a wider range of goods and services around the world. One could easily search for desired goods, place an order and then pay for it at the tips of their fingers on their devices within seconds (Casalini & López González, 2019). Thus, as the digital economy progresses, international instruments aiming to safeguard privacy across national borders are much needed.

There are many challenges on data privacy regarding the collection, transfer and use of personal data across international boundaries. Data users are concerned on the ambiguity on the usage and processing of data collecting without knowledge from data users. These could affect transmitting of data which is vital for small and medium-size enterprises (SMEs) engagement in trade.

Currently, there is lack of globally accepted binding multilateral rules between nations on how to regulate data across borders (Fefer, 2020, p. 28). This is because each country has its own national law on data policies. Countries like the EU are binding under the General Data Protection Regulation (GDPR), which focuses on user privacy. Meanwhile, law in China emphasises national security. These major differences cause challenges for businesses to operate internationally as online privacy regulations pose barriers for international trade. Law and policymakers need to create laws that balance the need for privacy and maintain open digital trade to ensure growth of the global economy.

Besides, business organisations involved must ensure they comply with these varying legal requirements on data privacy laws and regulations. They need to implement and adapt to each jurisdiction's laws in which they operate. For example, some countries may require data that could only be stored locally, which restricts them from offering services in certain regions. Different countries require different standards for data subject consent, rights and security protocols, which can be quite challenging for businesses with small capital and limited resources. Non-compliance with the local rules can lead to punishment, fines and reputational damage to the business. Failure of businesses to protect consumer rights could also face backlash as consumers lose trust and stop using certain platforms or websites.

6.1 Enforcement and Consumer Redress

Due to inadequacy in legal frameworks and a lack of awareness among consumers, the enforcement of consumer rights in the digital era faces several challenges and hindrances. It also limits consumer protection, making effective dispute resolution difficult, particularly in the realm of online privacy.

While the Malaysia PDPA imposes a number of legal obligations on data users, its effectiveness mostly depends on robust enforcement and compliance by corporations (Thetbanthad et al., 2025). The major challenge lies in enforcing the Tribunal for Consumer Claims, where businesses refuse to comply the awarded compensation. Majority of online services lack consideration towards data protection regulations which further complicates the problem (Liu et al., 2022). Besides, the PDPA does not cover all types of data processing and is limited to the private sector only. These limitations create loopholes in the law, which can hinder data protection, causing more data breaches. The broad nature of online and cross-border transactions makes it challenging to apply Malaysian laws outside the country.

Besides, the lack of resources for data protection is also an obstacle. Regulatory bodies often have limited financial aid and human resources, slowing down their ability to monitor compliance effectively (Alibeigi et al., 2021). As business organizations might not have trained personnel in enforcing privacy regulations, many of them struggle to keep pace with the rapid technology developments, along with the ever-evolving tactics to misuse personal data. Cross-border online transactions also create challenges if there are data breaches, for example in obtaining evidence and coordinating with foreign law enforcement agencies in the process.

Consumers in Malaysia also faces hurdles in the process of seeking redress for online privacy violations as most are unaware of their rights or lack the resources to seek legal action. Most even perceive online privacy violations as annoying and brushes it off instead of treating it as a serious breach of right issue (Ruschemeier, 2023). The process of filing a complaint and cost of legal representation sometimes deter consumers from seeking justice for themselves. The lack of a comprehensive data protection adds to the complications in seeking redress for privacy violations. Technology advancements bring more cybercrimes, which targets banking and e-commerce platforms, making it even complicated when it comes to seeking remedies for online privacy infringements.

It is undeniable the enforcement of consumer rights in Malaysia faces significant challenges due to gaps in the legal framework, limited enforcement capacity and lack of consumer awareness. These challenges prove to be problems that arise from cross-border data flows. Addressing them is vital for both SDG 9 and 16, which promotes rule of law in data governance. Businesses need to ensure they comply with national approaches to data privacy to maintain customer trust. As data plays a pivotal role in modern digital trade and communication, it is essential that there is a need to balance interests of privacy and promoting e-commerce. The lack of effective enforcement mechanisms and corporate compliance further weakens consumer protection regarding online privacy. Thus, Malaysia

must strengthen its legal and institutional frameworks, enhance cross-border cooperation and promote public education on digital rights and privacy to ensure meaningful protection for individuals in the digital era. An evolving policy landscape is needed to provide for different national perspectives of different countries.

7. The PDPA versus GDPR

Both the Malaysian PDPA and the EU GDPR are frameworks established to protect privacy and processing of personal data. However, when the research compares the PDPA to the GDPR, there are a few things the PDPA can refer to the GDPR for improvement.

The General Data Protection Regulation (GDPR), enacted on 25 May 2018 across the European Union (EU) replaced the Data Protection Data Protection Directive 95/46/EC (DPD) (European Data Protection Supervisor, n.d.). It is also known as the golden standard for data protection. It strengthens data protection and business opportunities in the digital market. Compared to the PDPA in Malaysia, data subjects within the EU have stronger control over their personal data. The PDPA also appears to be less stringent in comparison. Section 3(2) of the PDPA limits its applicability as it is only applicable to Malaysia's jurisdiction. Meanwhile, the GDPS applies to data controllers and processors in the EU, also extending to organisations processing data of EU residents. This means that the GDPR has a wider jurisdiction.

The PDPA in Malaysia is applicable to commercial transactions in the private sector only, while the GDPR provides extensive coverage to personal data regardless of its nature. This raises concerns because of the lack of protection for non-commercial data. This also means that the GDPR grants rights to data subjects more than the GDPR.

The next key difference would be the right to data portability which allows individuals to obtain and reuse their personal data for their own purposes across different services. There is no such provision however in the PDPA, but Article 20 of the GDPR provides that data subjects have such a right to receive personal data concerning themselves. As the PDPA applies to business transactions only, such a right may not be needed as data subjects have the choice to transfer their data to other businesses out of free consent.

The European Data Protection Authorities (DPA) can impose fines up to 4% of a company's annual revenue for violations of its regulations (Wolff & Atallah, 2021), although inconsistent across its member states. Comparatively, the Malaysian PDPA has a relatively lower fines, ranging from RM100,000.00 to RM500,000 with imprisonment, depending on the specific violation (Prasetyoningsih et al., 2024). DPAs, with the enforcement of GDPR has been giving warnings, fines and processing limitations, leading to the significant increase of public awareness and corporate accountability on data privacy. While the Malaysian PDPA mandates that data users safeguard data collected and to align with data protection principles, enforcement has been less compared to the GDPR (Alibeigi et al., 2021), where the available policy implementations are mostly hindered by political and infrastructural challenges (Mohamad et al., 2025). This means that the GDPR has a broader scope and more

stringent enforcement compared to PDPA which focuses on private sector and faces difficulties in public awareness and compliance, leading to the need for updates to meet current data protection demands.

Besides, both regulations provide different rights to data subjects. Under the EU's GDPR, data subjects have the right to be forgotten, where they could have businesses delete their personal information under specific circumstances. While in Malaysia, section 10 of the PDPA provides that businesses should not keep data for 'longer than necessary'. There is no time limitation for this stated anywhere. Thus, there have been suggestions that the PDPA needs better enhancement to provide stronger protection on confidentiality of an individual's personal data (Basarudin et al., 2017).

In Malaysia, the application of the PDPA has been considered to be a 'mystery', and it may not meet the standards of developed regions like the EU's GDPR (Sureani et al., 2021). For example, as the EU applies even to data of EU residents processed outside the EU, the PDPA does not recognise extraterritorial jurisdiction. Aligning the PDPA with international standards and introducing new methods and measures will provide better protection for data subjects in Malaysia.

When people tend to shop online more on different platforms, they are exposing themselves to a higher risk of the invasion of privacy online. Digital technology increases the opportunity for violations of the right to privacy. Malaysia does not have an expressed right to privacy except for violations of data usage for commercial transactions under the PDPA. This is because while both the GDPR and Malaysia's PDPA aim to protect personal data, the GDPR is more comprehensive. This research identifies a new lacuna in the current law regarding the right to privacy for digital commerce, and also the need for new regulations on personal data circulating on the respective online shopping platforms. Besides, suggestions shall also be made as to how the PDPA should be amended to protect the user's right to privacy online. By amending to align more closely with international standards and appointment of Data Protection Officers, Malaysia's PDPA could benefit and acquire more international investments.

7.1 Insights from Australia's Privacy Act 1988

In addition, Australia's Privacy Act 1988 (PA 1988) also offers valuable insights for Malaysia's PDPA. In contrast to the PDPA which primarily covers the private sector, the PA's coverage includes both the public and private sectors. Both serve as pivotal instruments in safeguarding consumer privacy within the digital sphere, especially concerning online shopping. The PA 1988 is influenced by the Guidelines Governing the Protection of Privacy and Transborder Flow of Personal Data adopted by Organisation for Economic Co-operation and Development (OECD). It provides international consensus on the collection and management and personal data, serving as a fundamental foundation for global privacy protection. Australia's PA 1988 offers broader and a more comprehensive protection for

consumers online, including right to access and complaint mechanisms (Othman & Samah, 2022).

Each Australian state and territory have their respective privacy legislation which mostly applies to public sector entities (Smith et al., 2021). Enforcement in Australia has broader powers to investigate and initiate inquiries whenever there are complaints. They are able to issue determination and enforceable undertakings, including referring serious breaches for criminal prosecution under the Criminal Code Act 1995. This means that Australia offers stronger enforcement mechanisms and broader rights for individuals, which also means more comprehensive consumer protection (Mohamed, 2012). They also enforce stricter transparency and consent rules. Meanwhile in Malaysia, studies have indicated that non-compliance on data protection, specifically in sectors handling sensitive data (Alibeigi & Munir, 2022). By strengthening consent machines and mandating clear privacy notifications in e-commerce, Malaysia can enhance consumer trust in online shopping.

Australia's Privacy Act 1988 also covers cross-border disclosures, ensuring overseas compliance. This extraterritorial application means that corporations are required to take reasonable steps in ensuring oversea recipients do not breach Australian Privacy Principle. The Office of the Australian Information Commissioner (OAIC) can act against entities that breach APPs, including cross-border disclosure breaches. This contrasts to Malaysian PDPA's limited jurisdictions which do not cover data processed outside Malaysia. Although Section 129 of the PDPA imposes specific conditions that must be met before international transfers are permitted, if there is any breach, the enforcement mechanism is limited to Malaysian jurisdiction only. It means that once the data leaves Malaysia successfully, the PDPA no longer governs its use.

Generally, as Australia's PA 1988 has a more comprehensive and stronger data protection framework, Malaysia could adopt its practices in areas like cross-border data governance and enforcement mechanisms. By adopting these lessons from Australia, Malaysia can improve its legal framework, enhance trust in online shopping and create a safer environment for data transmission in a rapidly growing digital economy.

8. Future Directions and Recommendations in Comparison to GDPR

To improve and enhance PDPA in providing better consumer privacy protection in Malaysia's e-commerce sector, Malaysia can learn from the GDPR by extending PDPA's jurisdiction to foreign entities processing personal data from Malaysia, which ensures better data protection. Article 20 of the GDPR allows data portability, which is the right for data subjects to receive and transfer data between data controllers. By implementing this right into the PDPA, consumers have more control over the data, where they have the freedom to switch services from one platform to another, like from Shopee to Lazada without losing digital footprints. In this way, consumers feel more secure knowing that they have the freedom to move and control their data. This also mitigates fear of permanent data retention, reducing users' concerns when using online services. It also aligns Malaysia with global data

protection standards, which encourages cross-border commerce. It also makes Malaysia a more trusted digital hub for international companies.

Under the GDPR, Data Protection Impact Assessments (DPIA) are mandatory for new high risks transactions. It is to identify risks from data processing and to minimise them. It also enhances communication about data privacy and its risks to the public, improving and inspiring confidence in the public regarding online shopping. The PDPA should require all e-commerce platforms in Malaysia to conduct DPIAs before any large-scale data processing. Businesses will have to assess risks before launching any new product or service, for example biometric data leaks for platforms planning to use AI-facial recognition on respective platforms. This also encourages responsible AI and technology use, prevents systemic data abuse, and protects consumers from privacy harm.

Apart from referring to the GDPR, these reforms or amendments must also consider Malaysia's commitment to global sustainability. By strengthening the PDPA, Malaysia caters to SDG 9 by balancing privacy protection with technological advancement. In 2015, the United Nations adopted 17 Sustainable Development Goals (SDGs) as a universal call to action to end poverty, protect the planet, and ensure that by 2030 all people enjoy peace and prosperity. All the 17 SDGs are integrated as it is recognised that development of a nation must have a balance of all three aspects of social, economic and environmental sustainability (UNDP, n.d.). Among the 17 goals, Goal 9 which seeks to build resilient infrastructure, promote sustainable industrialization and foster innovation seems to align with the importance of having comprehensive data protection laws in the era of digital economy. Goal 9.1 seeks to 'develop quality, reliable, sustainable and resilient infrastructure, including regional and transborder infrastructure, to support economic development…' which can be seen from how the PDPA ensures the secure processing of personal data in e-commerce transactions. This would encourage trust from the users in digital platforms and infrastructure which is essential in promoting inclusive and sustainable industrialization, a key target of SDG 9. Besides that, Goal 9.2's aim 'to promote inclusive and sustainable industrialisation' is reflected in the recently amended Section 43A as well as Section 129 of the PDPA which provides guidelines on rights to data portability and cross-border data transfers. These provisions safeguard and encourage global connectivity and access to technology which is essential in achieving Goal 9.2's target of inclusive infrastructure. In addition, the PDPA also aligns with Goal 9.4 which is to 'upgrade infrastructure and retrofit industries to make them sustainable…' as well as Goal 9.5 that encourage innovation by regulating data usage and protecting the customers' privacy and encouraging businesses to innovate responsibly (United Nations, n.d.).[2]

Moreover, the reforms should also align with SDG 16. SDG 16.6 focuses on developing effective, accountable and transparent institutions at all levels, including data protection. By emphasizing organizational accountability for data breaches, digital transformation enhances efficiency and transparency of online platforms, aligning with this SDG's target for data protection, ensuring access to information and protecting fundamental rights. As both

[2] https://www.un.org/sustainabledevelopment/infrastructure-industrialization/

PDPA and the GDPR demands clarity on what data is collected and processed, transparency as a foundation for strong institutions and public trust is achieved. With the new Data Sharing Act 2025, the framework and guidelines for protecting public sector data exchange could be a model for private sector compliance with this SDG. As more platforms start to use AI in their platforms, it is important to note that they should be mandated to maintain transparency in AI decision-making processes and ensure non-discrimination, aligning with GDPR's principles and promoting justice and accountability (Kamaruddin et al., 2023). By reforming its legal and regulatory mechanisms, Malaysia can better conform to international norms and support peace, justice, and data privacy.

9. Conclusion

In conclusion, this study highlights the significance and importance of consumer data privacy protection in Malaysia's digital economy. The PDPA plays a vital role, providing the basic and important guidelines for safeguarding consumer data. To further enhance this, there are significant gaps for Malaysia to address so that it aligns with global standards and sustainable development goals. It is necessary for platforms to adopt proactive cyber security measures to prevent cyber threats and decrease the vulnerability of digital transactions. By referring to the GDPR and Australia's Privacy Act 1988, Malaysia can establish robust regulations and improvements for safer and better international data exchanges. Aligning data protection with international standards in Malaysia can transform Malaysia into a more trusted international digital hub, attracting international investments and cross-border digital trades. Malaysia's commitment to United Nation's sustainable development goals, specifically in fostering innovation and data protection as part of sustainable economic growth should also be taken into consideration in the reforms. All these suggestions and reforms together are practical and important practices, which contributes towards a more trustworthy and safer digital economy in Malaysia.

Acknowledgement

The author would like to express sincere appreciation to all individuals and institutions who have provided valuable support and assistance throughout the completion of this work. Special thanks are extended to those who contributed through technical assistance, data collection, and administrative support. The author is also grateful to those who offered helpful feedback and language editing.

The author also wishes to extend heartfelt thanks to the Faculty of Law, Universiti Teknologi MARA (UiTM), and Universiti Malaya for their institutional support and encouragement throughout this research.

Funding Statement

No funding was received.

Authors' Contributions

Lim: Led the conceptualisation and development of the research framework. Contributed to the methodology, data curation, and formal analysis. Prepared the original draft of the manuscript and participated in writing – review and editing. Shared supervision responsibilities.

Zulkifli: Contributed to the methodology, data curation, and formal analysis. Participated in writing – review and editing. Shared supervision responsibilities.

Conflict of Interest Declaration

The authors declare no conflict of interest.

Ethics Approval

This study did not involve human or animal subjects or personal data and therefore did not require ethical approval.

AI Usage Declaration

The author declares that Artificial Intelligence (AI) tools, which is QuillBot, was used solely to assist with language editing and paraphrasing during the preparation of this manuscript. These tools were not used to generate substantive content, ideas, or analysis presented in the work. All intellectual contributions, arguments, and conclusions are the author's own.

References

Adams, M. (2017). Big data and individual privacy in the age of the Internet of Things. *Technology Innovation Management Review*, *7*(4), 12–24. https://doi.org/10.22215/timreview/1067

Alibeigi, A., & Munir, A. B. (2022). A decade after the Personal Data Protection Act 2010 (PDPA): Compliance of communications companies with the notice and choice principle. *Journal of Data Protection & Privacy*, *5*(2), 119–137. https://doi.org/10.69554/YQUG8122

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 & Technology, *35*(3), 365–394. https://doi.org/10.1080/13600869.2021.1970936

Bakar, N. A., Rosbi, S., & Uzaki, K. (2020). E-wallet transactional framework for digital economy: A perspective from Islamic financial engineering. *International Journal of*

Management Science and Business Administration, *6*(3), 50–57. https://doi.org/10.18775/ijmsba.1849-5664-5419.2014.63.1005

Basarudin, N. A., Yeon, A. L., Mohamed Yusoff, Z., Md Dahlan, N. H., & Mahdzir, N. (2017). Smart home user's information in cloud system: A comparison between Malaysian personal data protection act 2010 and EU general data protection regulation. *Malaysian Construction Research Journal*, *2*(2), 209–222. https://www.cream.my/data/cms/files/MCRJ%20SI%20Vol%202%20No_2%202017.pdf#page=220

Beh, L. S. (2019, March 8–9). Digital economy: A paradise or threat in the new norm? [Conference presentation]. *4th Asia-Pacific Public Policy Network Conference* (AP-PPN 2019), Hong Kong, China. http://eprints.um.edu.my/id/eprint/20770

Bin Noor Azman, M. A., & Awang, M. N. (2020). Personal data protection of predictive analytics in online shopping: From Malaysian legal perspective. In *The 3rd International Conference of the Postgraduate Students and Academics in Syariah and Law 2020* (INPAC 2020) (pp. 78–86). https://oarep.usim.edu.my/entities/publication/87c79eee-f70d-4a54-9843-e013c7038b87

Casalini, F., & López González, J. (2019). *Trade and cross-border data flows* (OECD Trade Policy Papers, No. 220). OECD Publishing. https://doi.org/10.1787/b2023a47-en

Chua, H. N., Herbland, A., Wong, S. F., & Chang, Y. (2017). Compliance to personal data protection principles: A study of how organizations frame privacy policy notices. *Telematics and Informatics*, *34*(4), 157–170. https://doi.org/10.1016/j.tele.2017.01.008

Darmatama, M., & Erdiansyah, R. (2021). The influence of advertising in Tiktok social media and beauty product image on consumer purchase decisions. In *Proceedings of the International Conference on Economics, Business, Social, and Humanities* (ICEBSH 2021) (pp. 888–892). Atlantis Press. https://doi.org/10.2991/assehr.k.210805.140

European Data Protection Supervisor. (n.d.). *The history of the General Data Protection Regulation*. https://www.edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en

Fefer, R. F. (2020). *Data flows, online privacy, and trade policy* (Report No. 45584). Congressional Research Service. https://www.congress.gov/crs-product/R45584

Foerster-Metz, U. S., Marquardt, K., Golowko, N., Kompalla, A., & Hell, C. (2018). Digital transformation and its implications on organizational behavior. *Journal of EU Research in Business*, Article 340873. https://doi.org/10.5171/2018.340873

Gelman, L. (2009). Privacy, free speech, and blurry-edged social networks. *Boston College Law Review*, *50*(5), 1315–1344. https://bclawreview.bc.edu/articles/953

Green, J. (2022). Cybersecurity challenges in the digital age. *International Multidisciplinary Journal of Science, Technology & Business*, *1*(4), 19–23. https://imjstb.com/index.php/Journal/article/view/22

Groppe, S., Kuhr, F., & Coskun, M. A. (2018). Anonymous shopping in the Internet by separation of data. *Open Journal of Web Technologies*, *5*(1), 14–22. https://d-nb.info/1168144469/34

Hsu, C.-L., & Lin, J. C.-C. (2016). Exploring factors affecting the adoption of Internet of Things services. *Journal of Computer Information Systems*, *58*(1), 49–57. https://doi.org/10.1080/08874417.2016.1186524

Kamaruddin, S., Mohammad, A. M., Saufi, N. N. M., Rosli, W. R. W., Othman, M. B., & Hamin, Z. (2023). Compliance to GDPR data protection and privacy in artificial intelligence technology: Legal and ethical ramifications in Malaysia. In 2023 *International Conference on Disruptive Technologies (ICDT)* (pp. 284–288). IEEE. https://doi.org/10.1109/ICDT57929.2023.10150615

Kosimov, J., & Ruziboyeva, G. (2022). The role of the digital economy in the world. *Scientific Progress*, *3*(2), 435–441. https://cyberleninka.ru/article/n/the-role-of-the-digital-economy-in-the-

Liu, Z., Iqbal, U., & Saxena, N. (2022). *Opted out, yet tracked: Are regulations enough to protect your privacy?* ArXiv. https://doi.org/10.48550/arXiv.2202.00885

Malaysian Communications and Multimedia Commission. (2024). *Internet users survey 2022*. https://www.mcmc.gov.my/skmmgovmy/media/General/IUS-2022.pdf

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. In *International Conference on Medical Imaging, Electronic Imaging, Information Technologies, and Sensors (MIEITS 2025)* (Vol. 13631, pp. 189–196). SPIE. https://doi.org/10.1117/12.3059023g

Mohamed, D. B. (2012). Sustaining the right to privacy in e-commerce environment: The legal approach. *OIDA International Journal of Sustainable Development*, *5*(1), 97–106. http://oidaijsd.com/wp-content/uploads/2019/04/05-01-10.pdf

Othman, M. B. B., & Samah, M. F. B. A. (2022). The Australian Privacy Act 1988: Lesson to be learned. *Malaysian Journal of Social Sciences and Humanities (MJSSH)*, *7*(9), Article e001766. https://doi.org/10.47405/mjssh.v7i9.1766

Polyakov, M., & Kovshun, N. (2021). Diffusion of innovations as a key driver of the digital economy development. *Baltic Journal of Economic Studies*, *7*(1), 84–92. https://cyberleninka.ru/article/n/diffusion-of-innovations-as-a-key-driver-of-the-digital-economy-development

Prasetyoningsih, N., Ismail Nawang, N., Putri, W. V., & Amirullah, M. N. R. (2024). Legal protection for the personal data in Indonesia and Malaysia. In *International Conference on*

Human-Computer Interaction (pp. 161–169). Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-61379-1_11

Ramaiah, A. K. (2019). Competition in digital economy: Fate of consumer welfare in Malaysia. *Malaysian Journal of Consumer and Family Economics*, *22*(S1), 223–245. https://www.majcafe.com/competition-in-digital-economy-fate-of-consumer-welfare-in-malaysia/

Robinson, S., Chai, W., & Stedman, C. (2023, December 20). *Big data analytics*. Business Analytics. https://www.techtarget.com/searchbusinessanalytics/definition/big-data-analytics

Ruschemeier, H. (2023). Data brokers and European digital legislation. *European Data Protection Law Review*, *9*(1), 27–38. https://doi.org/10.21552/edpl/2023/1/7

San, T. P. (2020). Predictions from data analytics: Does Malaysian data protection law apply? *Information & Communications Technology Law*, *29*(3), 291–307. https://doi.org/10.1080/13600834.2020.1759276

Segado-Boj, F., & Díaz-Campo, J. (2020). Social media and its intersections with free speech, freedom of information and privacy: An analysis. *Icono 14*, *18*(1), 231–255. https://www.redalyc.org/journal/5525/552562132011/html/

Sidi Ahmed, S. M., & Zulhuda, S. (2019). Data protection challenges in the Internet of Things era: An assessment of protection offered by PDPA 2010. *International Journal of Law, Government and Communication*, *4*(17), 1–12. https://doi.org/10.35631/ijlgc.417001

Smith, R. B., Perry, M., & Smith, N. N. (2021). Three shades of data: Australia, Philippines, Thailand. *Singapore Journal of Legal Studies*, (1), 76–99. https://heinonline.org/HOL/P?h=hein.journals/sjls2021&i=77

Sureani, N. B. N., Qurni, A. S. B. A., Azman, A. H. B., Othman, M. B. B., & Zahari, H. S. B. (2021). The adequacy of data protection laws in protecting personal data in Malaysia. *Malaysian Journal of Social Sciences and Humanities*, *6*(10), 488–495. https://doi.org/10.47405/mjssh.v6i10.1087

Thetbanthad, P., Sathanarugsawait, B., & Praneetpolgrang, P. (2025). Automated redaction of personally identifiable information on drug labels using optical character recognition and large language models for compliance with Thailand's Personal Data Protection Act. *Applied Sciences*, *15*(9), Article 4923. https://doi.org/10.3390/app15094923

UNDP. (n.d.). *What are the Sustainable Development Goals?*. https://www.undp.org/sustainable-development-goals

United Nations. (n.d.). Goal 9: *Build resilient infrastructure, promote sustainable industrialization and foster innovation*. Sustainable Development Goals. https://www.un.org/sustainabledevelopment/infrastructure-industrialization/

Wolff, J., & Atallah, N. (2021). Early GDPR penalties: Analysis of implementation and fines through May 2020. *Journal of Information Policy*, 11, 63–103. https://doi.org/10.5325/jinfopoli.11.2021.0063

Xian, C. Y., Chua, W. H., Chua, C. J., Chuah, Y. C., Tan, M. N., Azzabilla, A., Risky, A. F., Oktavianti, A., & Ramadani, M. G. P. (2023). How online shopping on Shoppe platform affects the consumer behavior in Malaysia: An exploratory survey. *Journal of the Community Development in Asia*, *6*(3), 414–426. https://doi.org/10.32535/jcda.v6i3.2548

Yuvaraj, S., & Sheila Eveline, N. (2018). Consumers' perception towards cashless transactions and information security in the digital economy. *International Journal of Mechanical Engineering and Technology*, *9*(7), 89–96. https://iaeme.com/MasterAdmin/Journal_uploads/IJMET/VOLUME_9_ISSUE_7/IJMET_09_07_010.pdf

(This page is intentionally left blank.)