



DOI: <https://doi.org/10.38035/gijlss.v4i2>  
<https://creativecommons.org/licenses/by/4.0/>

## Data Commercialization in Cybersecurity Law and Policy: A Comparative Study of Indonesia and Malaysia

Hanifah Ghafila Romadona<sup>1\*</sup>, Mimi Sintia Mohd Bajury<sup>2</sup>, Febri Jaya<sup>3</sup>, Stefanus Eko Prasetyo<sup>4</sup>, Haeruddin<sup>5</sup>

<sup>1</sup>Universitas Internasional Batam, Batam, Indonesia, [hanifah@uib.ac.id](mailto:hanifah@uib.ac.id)

<sup>2</sup>Universiti Teknologi Mara, Selangor, Malaysia, [mimisintia@uitm.edu.my](mailto:mimisintia@uitm.edu.my)

<sup>3</sup>Universitas Internasional Batam, Batam, Indonesia, [Febri.jaya@uib.edu](mailto:Febri.jaya@uib.edu)

<sup>4</sup>Universitas Internasional Batam, Batam, Indonesia, [stefanus@uib.ac.id](mailto:stefanus@uib.ac.id)

<sup>5</sup>Universitas Internasional Batam, Batam, Indonesia, [haeruddin@uib.ac.id](mailto:haeruddin@uib.ac.id)

\*Corresponding Author: [hanifah@uib.ac.id](mailto:hanifah@uib.ac.id)<sup>1</sup>

**Abstract:** The rapid development of the digital economy has accelerated the commercialization of personal data in Indonesia and Malaysia, raising significant concerns regarding cybersecurity and consumer protection. This study aims to analyze and compare the legal frameworks governing data commercialization in both countries, particularly Indonesia's Personal Data Protection Law and Malaysia's Personal Data Protection Act 2010. Using a normative juridical and comparative approach, the study examines regulations related to consent, transparency, consumer rights, and law enforcement. The findings indicate that although both countries have established legal protections for personal data, major challenges remain in implementation, supervision, and enforcement. Weak transparency, unclear consent mechanisms, limited institutional oversight, and inadequate sanctions continue to create risks of personal data misuse and privacy violations. Furthermore, the imbalance of power between corporations and consumers often limits individuals' control over their personal information. This study concludes that stronger legal enforcement, improved transparency, enhanced consumer awareness, and collaboration between governments, corporations, and society are necessary to ensure effective consumer data protection and create a safer digital ecosystem in Indonesia and Malaysia.

**Keywords:** Data Commercialization, Indonesia, Malaysia, Personal Data Protection.

### INTRODUCTION

Indonesia, with its large digital population, stands as one of the key markets for the growth of financial technology (fintech), which not only includes digital payment services but also online lending and peer-to-peer (P2P) lending (Jange et al., 2024).

Data refers to information that can be collected, analyzed, and used for various purposes, including business, research, and policymaking (Weley & Disemadi, 2022). According to a report from Indonesia's Ministry of Communication and Informatics

(Komdigi), which recorded more than 1,000 data breaches in Indonesia in 2020, combined with findings from CNBC Indonesia indicating that approximately 10%–15% of data breaches were caused by negligence and outdated systems, as well as Surfshark data estimating that Indonesia contributes around 5%–10% of global data breaches, it is projected that data breaches in Indonesia may increase by approximately 10%–15% in 2024 and 2025 without significant improvements in data security systems (Wibowo et al., 2024). In the context of personal data protection, the 1945 Constitution of the Republic of Indonesia (The 1945 Constitution) provides a constitutional foundation recognizing every citizen's right to the protection of their personal data. Article 28G of the Constitution affirms that every individual has the right to personal protection, protection of family, honor, dignity, and property, as well as the right to feel secure from threats that undermine their fundamental rights (Wijaya & Gusliana, 2024). This constitutional guarantee also encompasses the protection of personal data utilized for both commercial and governmental purposes (Novri et al., 2023).

Cases of data commercialization in Indonesia and Malaysia reflect rapidly evolving challenges and opportunities in the digital era. In Indonesia, data breaches have become a major concern, with CNBC Indonesia reporting that many incidents are caused by technical failures and human negligence, resulting in improper data management and unauthorized use of leaked information. In this regard, Indonesia's Personal Data Protection Law (PDP Law), particularly Article 28, serves as the legal foundation for safeguarding individual privacy rights and regulating the protection of personal data (Prasteyoningsih et al., 2024). Meanwhile, in Malaysia, data mining has emerged as a significant issue because, although it is not inherently illegal, it may violate the law when personal data is collected and analyzed without adequate consent, particularly in the context of non-transparent data commercialization practices. This matter is regulated under Malaysia's Personal Data Protection Act (PDPA), specifically Section 6, which requires personal data to be collected with the consent of the individual concerned. On the other hand, Malaysia's data center market is projected to reach US\$4.04 billion in 2024 and exceed US\$13.5 billion by 2030, supported by substantial investments from North American hyperscaler companies amounting to US\$23.3 billion in 2024. This development demonstrates the rapid growth of digital infrastructure that facilitates large-scale data management and accelerates data commercialization in Malaysia (Kanojia & Zahra, 2025).

Several previous studies provide an important foundation for understanding issues related to personal data protection and relevant legal regulations. Severius Waruwu et al. (2022) analyzed the importance of harmonizing trade secret law and personal data protection law in Indonesia by positioning personal data as business information requiring dual protection, while emphasizing the need for an integrated legal framework to ensure legal certainty and safeguard both individual rights and corporate interests (Waruwu & Siswoyo, 2024). Furthermore, Rahmat Shodiq et al. (2022) proposed a civil law construction recognizing personal data as an object of property rights in commercial transactions by introducing a personal data protection model based on property law principles, aimed at providing greater legal certainty and addressing the imbalance of power between individuals and digital business actors in Indonesia (Rahmat et al., 2022).

Furthermore, Iwan Setiawan et al. (2022) criticized the practices of unauthorized airtime deduction and spam messages in Indonesia's telecommunications industry, arguing that automatic service registration without consent constitutes an abuse of circumstances, while spam messages represent unlawful processing of personal data (Kurnia et al., 2022). The study emphasized that mobile operators should bear strict liability for failures in data security systems and financial losses suffered by consumers, in accordance with Law Number 8 of 1999 concerning Consumer Protection and the PDP LAW. In addition, the study

conducted by Annisa Khoerotun Zahro et al. (2022) is also relevant, as it examined the ethics of endorsement practices by digital influencers on TikTok and identified the prevalence of “hidden advertising” without clear disclosure due to weaknesses in the Indonesian Advertising Ethics regulations (EPI) (Zahro et al., 2025). The study recommended policy reformulation through explicit disclosure obligations, independent supervision, and industry education to establish a more transparent and ethical digital communication ecosystem. Collectively, these studies provide comprehensive insights into the challenges of regulating personal data protection and highlight the urgent need for a more transparent and effective legal framework in Indonesia.

The novelty of this study lies in its comparative analysis of Indonesia and Malaysia regarding data commercialization and cybersecurity law and policy. This research examines two primary research questions: first, how data commercialization is regulated in Indonesia and Malaysia; and second, how consumer protection is ensured through data commercialization practices in both countries. Unlike previous studies that primarily focused on personal data protection and ethical issues within the digital industry, this study explores how both countries regulate data commercialization within a broader legal framework and examines its impact on consumers. In addition, this study evaluates the effectiveness of existing policies in providing consumer protection, particularly in terms of transparency, data security, and data access rights. The main objective of this research is to analyze and compare the regulatory frameworks governing data commercialization in Indonesia and Malaysia, while also assessing how these policies can effectively protect consumers in the digital economy era.

## **METHOD**

The theoretical significance of this study lies in enriching the existing literature on data commercialization, consumer protection, and cybersecurity policy, particularly in Indonesia and Malaysia, while also providing a deeper understanding of how both countries regulate data commercialization in the digital era (Disemadi, 2021). This study further contributes to the development of legal theories concerning the relationship between data commercialization and consumer protection, an area that has not been comprehensively explored in previous research (Tan, 2021). Through a comparative analysis of Indonesia and Malaysia, this study is expected to offer new insights into cyber law and policy that are relevant to the rapid development of the digital economy. From a practical perspective, this research is expected to serve as a reference for policymakers and regulators in formulating more holistic and comprehensive policies governing data commercialization and consumer protection. The findings of this study may assist the governments of Indonesia and Malaysia in developing regulations that are more adaptive to the digital economy, strengthening personal data protection, and creating a safer and more transparent digital ecosystem for consumers. The contribution of this research lies in offering a new perspective that holistically connects data commercialization, cybersecurity policy, and consumer protection within a broader legal and regulatory framework.

## **RESULTS AND DISCUSSION**

### **Data Commercialization Regulations in Indonesia and Malaysia**

Data commercialization has become a crucial issue in the digital era, as data is now considered a valuable asset traded across various sectors, including marketing, advertising, and product development. In Indonesia and Malaysia, data commercialization plays a significant role in supporting the growth of the digital economy, with many companies relying on consumers’ personal data as part of their business strategies (Disemadi, 2021). Both countries face significant challenges in regulating the use and protection of personal

data. The massive collection and distribution of data have increased the risks of misuse and violations of consumer privacy, often without users’ awareness (Tan, 2021). Indonesia has enacted the PDP LAW, while Malaysia regulates personal data protection through the Personal Data Protection Act (PDPA); however, the supervision and enforcement of these regulations remain weak (Farhan et al., 2022). Many companies have yet to fully comply with personal data protection regulations, while consumers are often not provided with sufficient transparency regarding how their data is collected, processed, and utilized. Stronger policies and more effective supervisory mechanisms are therefore required to ensure that data commercialization prioritizes privacy rights and consumer protection while simultaneously supporting sustainable digital economic growth in both countries (Kusnadi, 2021).

Meanwhile, in Malaysia, data commercialization is regulated under the Personal Data Protection Act (PDPA), enacted in 2010. The PDPA provides a stronger legal foundation governing the collection, use, and disclosure of personal data by organizations and corporations. The regulation requires companies to obtain explicit consent from individuals before collecting and processing their personal data (Kanojia & Zahra, 2025). Although the PDPA establishes clear principles regarding personal data management, several shortcomings remain in its implementation. One major issue is the weak supervision of large corporations engaged in large-scale data collection activities. Insufficient oversight has resulted in non-compliance with regulatory obligations and increased risks of personal data misuse, thereby weakening consumer protection. Furthermore, although companies are obligated to report data breaches, the existing sanction mechanisms are often considered inadequate in creating a sufficient deterrent effect against violations (Chong et al., 2024).

Both Indonesia and Malaysia also face challenges in regulating how personal data obtained from consumers may be traded or utilized for commercial purposes without violating individual privacy rights (Syailendra et al., 2024). The use of data for targeted advertising and market analysis is often conducted without the explicit consent of consumers, potentially infringing upon their privacy rights. This situation raises concerns regarding the extent to which corporations may exploit personal data for commercial gain without providing consumers with adequate control over their information. In Indonesia, although the PDP LAW requires explicit consent, many companies still lack transparency in the methods by which they collect and process personal data (Fachri & Dewi, 2024). Similarly, in Malaysia, although the PDPA regulates data collection based on consumer consent, its practical implementation remains insufficiently strict, resulting in the frequent use of consumer data for commercial purposes without clear notification. Such practices raise critical questions regarding the adequacy of personal data protection and whether consumers genuinely possess meaningful control over their personal information (Wiraguna, 2025).

**Table 1. Comparison of Indonesia and Malaysia Legal Framework**

Aspect	Indonesia	Malaysia
Main Legal Framework	PDP LAW and regulations related to electronic transactions, particularly Article 4 and Article 20 of the PDP LAW concerning personal data rights and consent for data processing	PDPA 2010, particularly Section 6 concerning consent requirements for personal data processing
Regulatory Focus	Personal data protection, consent for data processing, rights of data subjects, and obligations of data controllers as regulated under Articles 4–16 and Article 20 of the PDP LAW	Collection, use, disclosure, and storage of personal data by commercial organizations under Sections 6, 7, and 8 of the PDPA
Data Commercialization	Not specifically regulated as a separate legal regime, but limited through principles of consent, transparency, and purpose limitation	Regulated within the scope of personal data usage by the commercial sector, primarily through consent and

	in data processing under Articles 20, 21, and 65 of the PDP LAW	notification principles under Sections 6 and 7 of the PDPA
Consumer Consent	The use of data for commercial purposes must be based on valid and explicit consent from the data owner under Article 20 of the PDP LAW	The use of personal data for commercial purposes requires consent from the data subject under Section 6 of the PDPA
Transparency in Data Usage	Companies are required to explain the purpose of data collection and usage under Articles 21 and 22 of the PDP LAW, although implementation often lacks transparency	The PDPA requires notification regarding the purpose of data usage under Section 7 of the PDPA, but supervision of commercial practices remains a challenge
Use in Digital Marketing	Frequently used for targeted advertising, market analysis, and service personalization, but vulnerable to misuse without explicit consent as prohibited under Article 65 of the PDP LAW	Used for marketing and digital advertising, although regulatory gaps in overseeing corporate data usage still exist under Sections 43 and 129 of the PDPA
Consumer Rights	Consumers have the right to know, access, correct, and withdraw consent regarding the use of their personal data under Articles 5, 6, 7, and 8 of the PDP LAW	Consumers have the right to access, correct, and object to the use of data for certain marketing purposes under Sections 30, 34, and 43 of the PDPA

Source: Author’s analysis

In the regulation of data commercialization, there remains significant ambiguity regarding who holds the authority to control data generated by users. In Indonesia, although the PDP LAW provides legal rights concerning personal data protection, issues such as explicit authorization for data sharing and transparency in data usage remain highly debated (Batubara et al., 2025). Consumers are often not provided with sufficient information regarding how their data will be processed or shared with third parties, limiting their ability to make informed decisions concerning their personal information. This situation raises concerns regarding the effectiveness of existing regulations in providing substantive consumer protection. Although the PDP LAW requires companies to obtain consumer consent before processing personal data, in practice, clear and transparent consent mechanisms are still inadequately implemented. Furthermore, companies collecting and utilizing personal data frequently fail to transparently explain the purposes of data usage and the potential risks faced by consumers. Such ambiguity increases the risk of personal data misuse, ultimately undermining consumer privacy rights and weakening the effectiveness of personal data protection as regulated under the PDP LAW (Ramadhan, 2025).

In Malaysia the PDPA places greater emphasis on personal data control through fundamental principles governing the collection, use, and disclosure of data. The PDPA provides a clear legal framework regarding how personal data should be protected and establishes corporate obligations to obtain consumer consent prior to collecting personal information (Prasetyo et al., 2025). However, despite covering many essential aspects of personal data management, regulations concerning data commercialization, particularly in relation to digital advertising and online marketing, remain insufficiently strengthened. The use of personal data for digital marketing purposes is often conducted without adequate oversight, while companies frequently lack transparency regarding how personal information is utilized to target consumers through advertising. Furthermore, although the PDPA regulates the disclosure of personal data usage, supervision over corporations involved in digital marketing and advertising activities remains limited, thereby increasing the potential risk of data misuse and weakening consumer protection (Kurniawan et al., 2024).

One of the primary challenges in regulating data commercialization in both countries is the weakness of law enforcement mechanisms. In Indonesia, although regulations concerning electronic transactions and personal data protection have been enacted, their implementation

remains limited. While the PDP LAW recognizes consumer rights in relation to personal data protection, supervision and enforcement of these regulations remain weak, particularly within the commercial sector. This has resulted in numerous violations occurring without strict sanctions, including the collection of data without explicit consent and the non-transparent use of personal information. Consequently, consumers often feel inadequately protected and gradually lose trust in how corporations manage their personal data. Such legal uncertainty further exacerbates the issue, as consumers lack a sense of security regarding the commercial use of their personal information. Similarly, in Malaysia, although the PDPA provides a legal framework for personal data protection, weak oversight and insufficient enforcement of sanctions have contributed to comparable issues, thereby reducing the effectiveness of the regulation in ensuring adequate consumer protection (Shahidan, 2025).

Data commercialization also has significant implications for consumers, particularly regarding privacy rights. In Indonesia, although the PDP LAW grants individuals the right to control their personal data, the implementation of these rights remains far from optimal (Tania & Disemadi, 2024). Many consumers still lack a comprehensive understanding of how their data is collected, processed, and shared by corporations. The lack of transparency in these processes makes it difficult for consumers to effectively safeguard their rights. Furthermore, many companies fail to provide clear and sufficient information regarding the use of personal data, which further worsens consumer vulnerability. This situation contributes to limited public awareness concerning the potential risks associated with personal data misuse. Although the PDP LAW provides consumers with rights to access, correct, and delete their personal data, the practical implementation of these mechanisms remains limited, preventing consumers from fully exercising their rights. Therefore, more systematic and stringent measures are required to educate consumers and enhance corporate transparency in personal data management (Othman et al., 2021).

Personal data protection has become a central issue in the regulation of data commercialization. In Indonesia, although the PDP LAW provides a legal basis for protecting personal data, protection within commercial transactions remains insufficiently addressed within the existing regulatory framework (Zaki et al., 2023). Many companies collect personal data for marketing and advertising purposes without providing consumers with adequate information regarding how such data will be processed or shared. These practices are frequently conducted without the explicit consent of consumers, leaving individuals without meaningful control over their personal information. The lack of clarity in personal data management creates significant risks for consumers, as their data may be misused or commercially exploited without a clear understanding of the potential consequences. This situation highlights shortcomings in the implementation of the PDP LAW, which should provide more effective safeguards for personal data commercialization while strengthening corporate obligations to ensure transparency in consumer data management (Suhaimi et al., 2022).

In Malaysia although the PDPA establishes a legal framework for personal data protection, regulatory gaps still allow the misuse of personal information for commercial purposes. Many companies obtain consumers' personal data without clear consent or without providing adequate options for individuals to control how their information is utilized. This creates uncertainty for consumers regarding the use of their personal data, particularly in digital marketing and targeted advertising sectors. Although the PDPA requires companies to obtain consumer consent before collecting and processing personal data, the implementation of this principle is often insufficiently transparent and not clearly communicated to consumers. Without adequate mechanisms ensuring full consumer control over personal information, the potential for data misuse becomes significantly greater (Mudaa et al., 2021).

## **Consumer Data Protection within the Legal Politics of Cybersecurity and Data Commercialization in Indonesia and Malaysia**

Data commercialization in both countries is also closely connected to digital advertising, where companies utilize personal data to target consumers more specifically and strategically. In Indonesia, data-driven advertising frequently involves non-transparent practices, such as collecting user data through applications or websites without obtaining explicit consumer consent. Many consumers remain unaware that their personal information is being utilized for marketing purposes, as companies often fail to provide clear explanations regarding how such data is collected, processed, and exploited commercially. These practices raise serious concerns regarding the extent to which consumers can exercise control over their personal information in digital advertising ecosystems and whether adequate protection is provided against the commercial use of their data. The lack of transparency in the collection and utilization of personal data not only undermines consumer trust in corporations and digital platforms but also increases the risk of significant privacy violations and misuse of personal information (Prastyanti & Sharma, 2024).

Consumer data protection within the framework of cybersecurity law and data commercialization in Indonesia and Malaysia has become a major concern alongside the increasing use of personal data for commercial purposes. The collection, use, and distribution of personal data by various entities may create negative consequences for consumers, particularly when such data is misused or exposed without clear consent. These practices have the potential to undermine individual privacy rights, reduce consumer trust in corporations, and generate financial losses. In this regard, adequate personal data protection is essential to ensure that consumers maintain control over their information and are able to safeguard their privacy rights. As rapidly growing digital economies, both Indonesia and Malaysia face significant challenges in regulating how personal data is collected, processed, and protected, particularly within commercial sectors that heavily rely on data for marketing, advertising, and market analysis purposes (Rizal et al., 2024).

In Indonesia, consumer data protection is regulated under the PDP LAW enacted in 2022. The law grants consumers rights to control their personal data, including the rights to access, obtain information about, and delete data stored by corporations. Furthermore, the PDP LAW requires companies to obtain explicit consumer consent before utilizing personal data for commercial purposes, such as marketing and advertising. Although this regulation provides a stronger legal foundation for protecting consumer privacy rights, effective supervision and implementation remain significant challenges. Many companies still fail to fully comply with existing provisions, particularly regarding transparency in data processing and the establishment of clear consent mechanisms. In addition, the supervisory capacities of relevant institutions, such as the Komdigi and the National Cyber and Crypto Agency (BSSN), remain limited, resulting in many violations of personal data protection regulations not being followed by adequate sanctions. This situation raises concerns regarding the effectiveness of the PDP LAW in providing optimal consumer protection in Indonesia.

Meanwhile, in Malaysia, the PDPA serves as the primary legal framework for personal data protection. The PDPA provides clear safeguards for consumers, including the rights to access, correct, and delete their personal data, as well as the right to refuse the use of their data for marketing or advertising purposes. The regulation also establishes corporate obligations to obtain explicit consent before collecting and processing consumers' personal information. Although the PDPA provides a strong legal framework, weak supervision often reduces its effectiveness in protecting consumers. Many companies fail to comply with existing provisions, particularly by lacking transparency in explaining the purposes of data usage or by failing to provide clear mechanisms enabling consumers to control the use of their personal information. Furthermore, although the PDPA includes administrative

sanctions, inconsistent legal enforcement and the lack of independent oversight further weaken the effectiveness of personal data protection. As a result, consumers remain vulnerable to personal data misuse, ultimately reducing public trust in corporate data management practices.

**Table 2. Consumer Protection Between Indonesia & Malaysia**

Aspect of Consumer Data Protection	Indonesia	Malaysia
Consumer Rights over Personal Data	Under Articles 5–8 of the PDP Law, consumers have the right to access, correct, update, delete, and withdraw consent regarding their personal data.	Under Sections 30, 34, and 43 of the PDPA, consumers have the right to access and correct personal data and to refuse the use of their data for direct marketing purposes.
Consent and Consumer Control	Article 20 of the PDP Law requires companies to obtain explicit and informed consent before processing personal data.	Section 6 of the PDPA requires organizations to obtain consumer consent before collecting or processing personal data.
Transparency in Data Processing	Under Articles 21–22 of the PDP Law, companies are obligated to provide clear information regarding data collection, processing purposes, storage, and sharing with third parties.	Section 7 of the PDPA requires organizations to notify consumers about the purpose of data collection and processing, although many digital platforms still provide insufficient disclosure.
Protection Against Misuse of Consumer Data	The PDP Law prohibits unlawful disclosure, use, and transfer of personal data without consumer consent.	The PDPA prohibits the misuse and unauthorized disclosure of personal data by commercial organizations.
Law Enforcement and Consumer Protection Challenges	Consumer protection remains limited due to weak supervision by authorities such as Komdigi and BSSN, low public awareness, frequent data breaches, and inconsistent sanctions against corporations.	Enforcement by the Personal Data Protection Department (PDPD) faces challenges such as weak monitoring, limited transparency in corporate practices, and inconsistent enforcement against personal data violations.

Source: Author’s Analysis

Regulatory ambiguity also affects the implementation of explicit consent mechanisms. In Indonesia, although the PDP LAW requires companies to obtain consumer consent before processing personal data, consent procedures are often conducted in a non-transparent manner or through standard contractual clauses that do not provide consumers with clear choices. Many companies merely include consent provisions within lengthy and complex terms and conditions that are difficult for consumers to understand. In some cases, consumers are not provided with sufficient options to refuse or determine how their data will be used. This situation creates uncertainty regarding consumer rights and the use of personal data, thereby weakening the protection intended under the PDP LAW. Because consent is frequently treated as part of an automatic process without granting consumers full control, the regulation is unable to provide adequate protection. Strengthening consumer protection, therefore, requires corporations to adopt greater transparency regarding the purposes and use of personal data while ensuring that consumer consent is explicit, informed, and easily understood.

In Malaysia, although the PDPA requires companies to obtain consumer consent before collecting personal data, the implementation of transparency principles remains problematic. Certain companies continue to collect data covertly, without providing clear or sufficient information regarding how personal data will be utilized for commercial purposes. Such practices commonly occur on digital applications, websites, and online platforms, where consumer data is collected without adequate disclosure or without providing clear options for consent. Moreover, many corporations fail to adequately inform consumers about potential

risks or the use of personal data for marketing and market analysis purposes. This lack of transparency diminishes consumers' ability to make informed decisions regarding their personal information and reduces trust in companies involved in data collection activities. To strengthen consumer protection, companies in Malaysia must ensure that consent mechanisms are implemented in a clear, explicit, and transparent manner while also providing consumers with adequate access to understand and control the use of their personal data.

Furthermore, consumer data protection in both countries is also influenced by the imbalance of power between consumers and large corporations that collect and control personal data. Many consumers lack sufficient understanding of their rights concerning personal information, making it difficult for them to adequately protect their data. The limited level of public education regarding personal data protection increases consumer vulnerability to non-transparent practices and potential data misuse by corporations. In addition, large corporations often possess greater power in collecting and utilizing personal data, while consumers exercise only minimal control over how their information is processed (Fatmawati et al., 2025). This imbalance is further aggravated by the fact that most consumers do not read or fully understand the terms and conditions attached to digital services, which frequently contain clauses permitting extensive data collection without offering meaningful alternatives to refuse consent. Addressing this issue requires stronger efforts to increase consumer awareness regarding personal data rights, as well as stricter regulations ensuring that consumers possess greater control over their information and receive more effective protection against data misuse (Rahardjo et al., 2025).

One of the most important aspects of consumer data protection is supervision and law enforcement. In Indonesia, although the PDP LAW imposes obligations to protect personal data, its implementation remains limited. Oversight of violations committed by corporations is often insufficiently strong, resulting in numerous data breaches occurring without adequate sanctions. Institutions responsible for supervision and law enforcement, such as Komdigi, frequently encounter challenges in conducting comprehensive oversight, particularly over large corporations engaged in large-scale data collection activities. Furthermore, slow reporting mechanisms and delayed legal enforcement create the perception among companies that violations carry no immediate consequences. This situation weakens the effectiveness of personal data protection in Indonesia and reduces consumer trust in the existing legal system. Strengthening supervisory capacity, implementing stricter sanctions, and ensuring faster and more transparent law enforcement are therefore essential to hold corporations accountable for the management of consumers' personal data.

Complaint mechanisms also constitute an important element of consumer data protection. In Indonesia, although consumers are able to submit complaints regarding data violations, the complaint process remains relatively complicated and insufficiently responsive. Many consumers experience difficulties in accessing complaint services or obtaining prompt responses from authorities (Kumar, 2024). In addition, the lack of transparency in complaint handling procedures contributes to consumer dissatisfaction. In Malaysia, although a more structured complaint system exists through the Personal Data Protection Department (Jabatan PDP), its effectiveness remains limited due to weaknesses in supervision and uncertainty regarding sanctions for violations. Unclear complaint procedures and slow responses from relevant authorities frequently cause consumers to feel inadequately protected. Moreover, despite the existence of complaint mechanisms, weak legal enforcement against data violations discourages many corporations from improving their data protection policies and practices (Anjawai et al., 2022).

To improve consumer data protection, consumer education regarding their rights is essential. In both Indonesia and Malaysia, many consumers still lack a comprehensive

understanding of their rights related to personal data management, including the rights to access, correct, and delete their personal information. This limited understanding makes it difficult for consumers to effectively protect their personal information and increases their vulnerability to data misuse by corporations (Marune & Hartanto, 2021). Therefore, educational programs aimed at increasing awareness of personal data protection are crucial in empowering consumers to make more informed decisions regarding their data. Such education may include information on how data is collected, processed, and protected, while also providing a clearer understanding of consumers' rights in managing their personal information. Through comprehensive educational initiatives, consumers will become better prepared to safeguard their data and make more informed decisions regarding consent for personal data usage, which may ultimately strengthen public trust in personal data protection systems in Indonesia and Malaysia (Arifin et al., 2021).

In addition, collaboration between governments, corporations, and society is essential to strengthen consumer data protection. Governments must cooperate with the private sector and the public to ensure that regulations concerning personal data management are effectively implemented and that consumers are granted clear rights to control their data. Such collaboration may involve the development of more inclusive policies that accommodate the interests of various stakeholders while ensuring that corporations comply with strict data protection standards. Governments must also play an active role in educating the public regarding the importance of protecting personal data, while corporations should be held accountable for transparency in the collection and use of consumer information. Society, as digital users, must also be empowered to better understand their rights and how to protect their personal information. Strong cooperation among these stakeholders can contribute to the creation of a safer and more transparent ecosystem for personal data management, thereby improving consumer protection and strengthening public trust in data security systems in Indonesia and Malaysia (Judijanto et al., 2024).

Overall, consumer data protection within the framework of cybersecurity law and data commercialization in Indonesia and Malaysia requires comprehensive improvements in regulation, supervision, education, and law enforcement (Weley & Romadona, 2026). Both countries must adopt stricter and more transparent policies that not only protect consumers' personal data but also ensure that corporations comply with existing regulations responsibly. Furthermore, strengthening independent and efficient supervisory mechanisms is essential to ensure the proper implementation of regulations. Consumers should also receive deeper education regarding their rights in managing personal data in order to make more informed decisions. Stronger law enforcement against personal data violations, accompanied by clear and fair sanctions, will enhance consumer trust and improve overall personal data protection. Through these measures, Indonesia and Malaysia can establish a safer, fairer, and more transparent digital ecosystem while providing consumers with greater security in facing the challenges of data commercialization in the digital era.

## **CONCLUSION**

Data commercialization within the framework of cybersecurity law and policy in Indonesia and Malaysia faces significant challenges, despite both countries having adopted personal data protection regulations, namely the PDP LAW in Indonesia and the PDPA in Malaysia. Weak supervision, ambiguity regarding explicit consent mechanisms, and the lack of transparency in the commercial use of personal data remain major issues in ensuring effective personal data protection. Furthermore, the imbalance of power between consumers and corporations controlling personal data often leaves consumers without adequate control over their personal information, thereby increasing public distrust toward corporate data management practices.

To strengthen consumer protection and establish a secure digital ecosystem, Indonesia and Malaysia must improve policies related to data commercialization by enhancing supervision and enforcing stricter legal sanctions against violations. In addition, both countries need to increase consumer awareness regarding their rights over personal data and improve transparency in the use of data for commercial purposes. These measures are essential to ensuring more effective personal data protection, granting consumers greater control over their information, and creating a fairer and safer digital environment for all stakeholders involved.

## REFERENCES

- Anjawai, N. B., Amboro, F. Y. P., & Hutauruk, R. H. (2022). Perbandingan Perlindungan Hukum Terkait Data Pribadi di Indonesia dan Jerman. *AL-MANHAJ: Jurnal Hukum Dan Pranata Sosial Islam*, 4(2), 207-218. DOI: <https://doi.org/10.70742/ajcos.v1i2.115>
- Arifin, R., Kambuno, J. A., Waspiyah, W., & Latifiani, D. (2021). Protecting the Consumer Rights in the Digital Economic Era: Future Challenges in Indonesia. *Jambura Law Review*, 3, 135-160. <https://jws.rivierapublishing.id/index.php/jws/article/view/584>
- Batubara, T. H., Marbun, A. S., Lubis, A. D., & Nirodi, M. A. (2025). Perspectives on Commercial Law Enforcement in the Era of Digitalization and Globalization. *Jurnal Sahabat ISNU SU*, 2(2), 26-30. DOI: <https://doi.org/10.70826/jsisnu.v2i2.817>
- Chong, S. Z., Kuek, C. Y., & Tay, E. S. (2024). Analysis of Image Rights Recognition in Malaysia: A Comparative Study with Selected Jurisdictions. *Pakistan Journal of Life & Social Sciences*, 22(2). [http://www.pjls.edu.pk/pdf\\_files/2024\\_2/15130-15134.pdf](http://www.pjls.edu.pk/pdf_files/2024_2/15130-15134.pdf)
- Disemadi, H. S. (2022). *Lenses of Legal Research: A Descriptive Essay on Legal Research Methodologies*. *Journal of Judicial Review*, 24(2), 289–304. <https://doi.org/10.37253/jjr.v24i2.7280>
- Disemadi, H. S. (2021). Urgensi regulasi khusus dan pemanfaatan artificial intelligence dalam mewujudkan perlindungan data pribadi di Indonesia. *Jurnal Wawasan Yuridika*, 5(2), 177-199. DOI: <https://doi.org/10.25072/jwy.v5i2.460>
- Fachri, M., & Dewi, E. F. (2024). Personal Data Usage in Marketing Activity to Comply with PDP Law in Indonesian Digital Commerce Company (Case Study: PT Pitjarus Teknologi). *International Research Journal of Economics and Management Studies IRJEMS*, 3(1). <https://doi.org/10.56472/25835238/IRJEMS-V3I1P111>
- Farhan, F., Hamdani, F., Astuti, N. L. V. P., Fiqry, H. A. H., & Aulia, M. R. (2022). Reformasi hukum perlindungan data pribadi korban pinjaman online (perbandingan Uni Eropa dan Malaysia). *Indonesia Berdaya*, 3(3), 567-576. <https://ukinstitute.org/journals/ib/article/view/264>
- Fatmawati, E., Nury, A., Rafa, M. F. F., Sari, A. R., & Hasibuan, M. (2025). Digital Rights Regulation In The AI Era: Privacy Protection and Consumer Rights in Indonesia. *Journal of Social and Economics Research*, 7(2), 1780-1792. <https://idm.or.id/JSER/index.php/JSER/article/view/1344>
- Judijanto, L., Solapari, N., & Putra, I. (2024). An analysis of the gap between data protection regulations and privacy rights implementation in Indonesia. *The Easta Journal Law and Human Rights*, 3(01), 20-29. <https://esj.eastasouth-institute.com/index.php/eslhr/article/view/351>
- Kanojia, S., & Zahra, I. A. (2025). Economic Development and Privacy Regulations in Malaysia: The Case of PDPA 2010. In *Sustainable Smart Cities and the Future of Urban Development* (pp. 443-462). IGI Global Scientific Publishing. <https://www.igi-global.com/chapter/economic-development-and-privacy-regulations-imalaysia/364387>

- Kumar, S. (2024). Assessing the Impact of Indonesia's Personal Data Protection Law on E-commerce Consumer Rights. *Problematika Hukum*, 10(2), 117-131. <https://e-journal.president.ac.id/index.php/problematika-hukum/article/view/5626>
- Kurnia, G., Setiawan, I., Tridakusumah, A. C., Jaelani, G., Heryanto, M. A., & Nugraha, A. (2022). Local wisdom for ensuring agriculture sustainability: A case from Indonesia. *Sustainability*, 14(14), 8823. <https://www.mdpi.com/2071-1050/14/14/8823>
- Kurniawan, K. D., Hehanussa, D. J., Setiawan, R., Susilowati, I., & Helfisar, D. (2024). Criminal Sanctions and Personal Data Protection in Indonesia. *Lex Publica*, 11(2), 221-247. DOI: <https://doi.org/10.58829/lp.11.2.2024.255>
- Kusnadi, S. A. (2021). Perlindungan hukum data pribadi sebagai hak privasi. *AL WASATH Jurnal Ilmu Hukum*, 2(1), 9-16. DOI: <https://doi.org/10.47776/alwasath.v2i1.127>
- Marune, A. E. M. S., & Hartanto, B. (2021). Strengthening personal data protection, cyber security, and improving public awareness in Indonesia: Progressive legal perspective. *International Journal of Business, Economics, and Social Development*, 2(4), 143-152. <https://v2.rescollacomm.com/index.php/ijbesd/article/view/170>
- Mudaa, S., Mokhtar, M. Z., Aminc, W. A. A. M., Sofian, A., & Halimd, A. (2021). Developing Determinant Factors for Product Commercialization and Innovation in Malaysia. *International Journal of Innovation, Creativity and Change*, 15(9), 560-576. [https://www.ijicc.net/images/Vol\\_15/Iss\\_9/15944\\_Mokhtar\\_2021\\_EI\\_R.pdf](https://www.ijicc.net/images/Vol_15/Iss_9/15944_Mokhtar_2021_EI_R.pdf)
- Novri, N., Amboro, F. Y. P., & Hutauruk, R. H. (2023). A Analisis Perlindungan Konsumen Dalam Tindakan Penyalahgunaan Data Pribadi Oleh Penyelenggara Pinjaman Online Berdasarkan Perspektif Hukum Indonesia. *AL-MANHAJ: Jurnal Hukum Dan Pranata Sosial Islam*, 5(1), 547-556. DOI: <https://doi.org/10.37680/almanhaj.v5i1.2488>
- Prasetyoningsih, N., Ismail Nawang, N., Putri, W. V., & Amirullah, M. N. R. (2024, June). Legal Protection for the Personal Data in Indonesia and Malaysia. In *International Conference on Human-Computer Interaction* (pp. 161-169). Cham: Springer Nature Switzerland. [https://link.springer.com/chapter/10.1007/978-3-031-61379-1\\_11](https://link.springer.com/chapter/10.1007/978-3-031-61379-1_11)
- Rahmat, A., Imron, K., & Shodiq, M. J. F. (2022). Analisis Kesalahan Bahasa Arab Pada Judul Proposal Mahasiswa UIN Raden Fatah Palembang. *Kilmatuna: Journal of Arabic Education*, 2(2), 270-280. <http://ejournal.unsuda.ac.id/index.php/pba/article/view/78>
- Tan, D. (2021). Metode penelitian hukum: Mengupas dan mengulas metodologi dalam menyelenggarakan penelitian hukum. *Nusantara: Jurnal Ilmu Pengetahuan Sosial*, 8(8), 2463-2478. DOI <https://doi.org/10.31604/jips.v8i8.2021.2463-2478>
- Othman, I. W., Topimin, S., Ahmad, S. N. B., & Hasan, H. (2021). Driving the development of SMEs' entrepreneurs in the era of digitalisation: From the dynamic perspective of law enforcement in Malaysia. *International Journal of Accounting*, 6(37), 124-143. [https://www.researchgate.net/profile/Irma-Othman/publication/356718178\\_Driving\\_The\\_Development\\_Of\\_SMEs'\\_Entrepreneurs\\_In\\_The\\_Era\\_Of\\_Digitalisation\\_From\\_The\\_Dynamic\\_Perspective\\_Of\\_Law\\_Enforcement\\_In\\_Malaysia/links/62665e09bca601538b66dd0b/Driving-The-Development-Of-SMEs-Entrepreneurs-In-The-Era-Of-Digitalisation-From-The-Dynamic-Perspective-Of-Law-Enforcement-In-Malaysia.pdf](https://www.researchgate.net/profile/Irma-Othman/publication/356718178_Driving_The_Development_Of_SMEs'_Entrepreneurs_In_The_Era_Of_Digitalisation_From_The_Dynamic_Perspective_Of_Law_Enforcement_In_Malaysia/links/62665e09bca601538b66dd0b/Driving-The-Development-Of-SMEs-Entrepreneurs-In-The-Era-Of-Digitalisation-From-The-Dynamic-Perspective-Of-Law-Enforcement-In-Malaysia.pdf)
- Prasetyo, B., Handayani, I. G. A. K. R., & Sulistiyono, A. (2025). Data Protection Laws in Indonesia: Navigating Privacy in the Digital Age. *Side: Scientific Development Journal*, 2(1), 9-16. DOI: <https://doi.org/10.59613/petfxv64>
- Prastyanti, R. A., & Sharma, R. (2024). Establishing consumer trust through data protection law as a competitive advantage in Indonesia and India. *Journal of Human Rights, Culture and Legal System*, 4(2), 354-390. DOI: <https://doi.org/10.53955/jhcls.v4i2.200>

- Ramadhan, M. C. (2025). Living Law and the Digitalization of Communal Intellectual Property: The Dialectic of Customary Law and the National Data Center. *Jurnal Mahkamah: Kajian Ilmu Hukum dan Hukum Islam*, 275-290. DOI: <https://doi.org/10.25217/jm.v10i2.6643>
- Rizal, M., Rosadi, S. D., & Taryana, A. (2024). Legal Framework for Consumer Data Protection For Digital Business SMES in Indonesia. *Journal of Law and Sustainable Development*, 12(1), e2809-e2809. <https://ojs.journalsdg.org/jlss/article/view/2809>
- Rahardjo, T. M. S., Noerdjaja, H., Pambudi, G. E., & Prabowo, M. S. (2025). Consumer protection legal frameworks in indonesia: the challenges of e-commerce and data privacy. *Research Horizon*, 5(2), 119-128. <http://journal.lifescifi.com/index.php/RH/article/view/491>
- Syailendra, M. R., Lie, G., & Sudiro, A. (2024). Personal data protection law in Indonesia: challenges and opportunities. *Indon. L. Rev.*, 14, 175. [https://heinonline.org/hol-cgi-bin/get\\_pdf.cgi?handle=hein.journals/indolawrev14&section=13](https://heinonline.org/hol-cgi-bin/get_pdf.cgi?handle=hein.journals/indolawrev14&section=13)
- Shahidan, N. H., Abdul Latiff, A. S., & Abdul Wahab, S. (2025). Examining issues and challenges in the commercialization of university generated intellectual property rights in Malaysia. *ASEAN Entrepreneurship Journal (AEJ)*, 11(1), 25-39. <https://ir.uitm.edu.my/id/eprint/113511/>
- Suhaimi, N. S., Abdul Halim, M. A. S., & Hashim, H. A. (2022). Commercialization of academic research: assessing the perception of academicians at a public university in Malaysia. *Journal of Applied Research in Higher Education*, 14(1), 59-76. <https://www.emerald.com/jarhe/article/14/1/59/433506>
- Tania, S., Tan, D., & Disemadi, H. S. (2024). Urgensi Pengaturan Data dan Informasi Elektronik Sebagai Benda Tidak Berwujud Dalam Sistem Hukum Kebendaan di Indonesia. *JURNAL LEGISIA*, 16(2), 81-93. <https://conferenceproceedings.ump.ac.id/pssh/article/view/1544>
- Waruwu, S., & Siswoyo, A. A. (2024). Data pribadi sebagai aset bisnis: Sinergi hukum rahasia dagang dan perlindungan data. *Lex Lectio Law Journal*, 3(2), 118-129. <https://jurnalgrahakirana.ac.id/index.php/JLL/article/view/118>
- Weley, N. C., & Romadona, H. G. (2026). How Can Risk-Based Online Submission Systems Accelerate MSME Growth in Indonesia's Digital Economy. *Barelang Journal of Legal Studies*, 4(1). <https://journal.uib.ac.id/index.php/barjoules/article/view/11841>
- Weley, N. C., & Disemadi, H. S. (2022). Implikasi Hukum Pemasangan CCTV di Tempat Umum secara Tersembunyi terhadap Perlindungan Data Pribadi. *Amnesti: Jurnal Hukum*, 4(2), 79-93. DOI: <https://doi.org/10.37729/amnesti.v4i2.2151>
- Wibowo, A., Alawiyah, W., & Azriadi. (2024). The importance of personal data protection in Indonesia's economic development. *Cogent Social Sciences*, 10(1). <https://doi.org/10.1080/23311886.2024.2306751>
- Wijaya, P., & Gusliana, H. B. (2024). Relevansi Hak Privasi Dalam Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik Dengan Pasal 28 G Ayat 1 Undang-Undang Dasar Negara Republik Indonesia Tahun 1945. *Jurnal Ilmiah Wahana Pendidikan*, 10(22), 662-672. <http://www.jurnal.peneliti.net/index.php/JIWP/article/view/11126>
- Wiraguna, S. A. (2025). Strengthening the Functional Autonomy of Data Protection Officers Under Indonesia's PDP Law 2022: A Critical Legal and Institutional Review. *Public Sphere: Jurnal Sosial Politik, Pemerintahan dan Hukum*, 4(3). DOI: <https://doi.org/10.59818/jps.v4i3.2317>
- Zaki, N. A. M., & Hashim, F. M. (2023). Effective Process of Commercialization at the Research Institutions in Malaysia. *Journal of Advanced Research in Business and*

*Management*

*Studies*, 30(1),

45-57.

<https://www.akademiabaru.com/submit/index.php/arbms/article/view/4702>

Zahro, A. K., Nurafni, M. I., Yahya, S. N., & Handoko, D. (2025). Antara Kredibilitas dan Komersialisasi dalam Problematika Etika Praktik Endorsement oleh Influencer Digital. *Jurnal Ilmu Sosial dan Humaniora*, 1(3), 596-603.  
<http://indojurnal.com/index.php/jisoh/article/view/559>