Journal of Posthumanism
2025
Volume: 5, No: 3, pp. 138–152
ISSN: 2634-3576 (Print) | ISSN 2634-3584 (Online)
posthumanism.co.uk

DOI: https://doi.org/10.63332/joph.v5i3.465

User Registration Data for Strengthening Consumer Data Protection in Indonesian Digital MSMEs: A Malaysia Comparison

Yosia Hetharie[1], Isis Ikhwansyah[2], Ema Rahmawati[3],

Abstract

The protection of consumers' personal data is vital for the sustainability of digital MSMEs. Although Indonesia has Law No. 27 of 2022 on Personal Data Protection, the absence of mandatory data user registration creates gaps in supervision and compliance. This study analyzes the potential implementation of a data user registration system to strengthen personal data protection in Indonesia by comparing it with Malaysia, which has enforced such a system since 2013. This normative juridical study compares Indonesia's PDPR and Malaysia's PDPA to assess the role of data registration in MSME transparency and accountability. It finds that Malaysia's data user registration system strengthens personal data protection through stricter oversight, while Indonesia's lack of such a system may weaken supervision. The study recommends adopting a registration system in Indonesia to improve compliance, transparency, and data security for digital MSMEs.

Keywords: *Data User Registration, Personal Data Protection, Consumers, Digital MSMEs.*

Introduction

Indonesia's economic development is based on Pancasila economic democracy as an integral part of national development, encompassing economic, political, socio-cultural, and security aspects to achieve a just and prosperous society (Srikalimah *et al.*, 2020). Article 33 of the 1945 Constitution of the Republic of Indonesia (1945 Constitution) serves as the fundamental basis of the national economic system, emphasizing the principles of cooperation and mutual welfare rather than a capitalist economy based on individualism (Manan, 1995). With technological advancements, the Micro, Small, and Medium Enterprises (MSME) sector, as a key pillar of the economy, faces significant challenges (Soewardi, 1989). Data from the Ministry of Cooperatives and Small and Medium Enterprises in 2023 indicates that MSMEs account for 99.99% of all businesses in Indonesia, absorb 96.9% of the workforce, and contribute 60.05% to the GDP. However, MSME participation in the global value chain remains low at only 4.1%, and partnerships with large enterprises are limited to 7% (Kementerian Koperasi dan UKM, 2023). Moreover, there has been no significant shift in the scale of MSMEs over the past decade, leading to stagnation in business growth.

The transformation of MSMEs into the digital ecosystem is driven by advancements in information technology and the Fourth Industrial Revolution 4.0 (Wibowo, 2023), which integrates automation (Ekowati *et al.*, 2023), artificial intelligence (AI) (Fonna, 2019), and data analytics into business processes (Savitri, 2019). These changes enhance efficiency (Haqqi and

[1] Doctoral Program of Law Padjadjaran University, ochipull@ymail.com (Corresponding Author)
[2] Padjadjaran University, isis.ikhwansyah@unpad.ac.id.
[3] Padjadjaran University, ema.rahmawati@unpad.ac.id.

Wijayati, 2019), foster innovation (Cihuy, 2019) and improve the competitiveness of MSMEs in accessing broader markets across various sectors, such as manufacturing, transportation, and healthcare, thereby accelerating digital transformation worldwide (Deni, 2023).

Indonesia is currently adapting to Society 5.0 (Ifadhila *et al.*, 2024), which emphasizes the integration of technology (Dewa, 2022), with social life (Juwita and Handayani, 2022), to create sustainable solutions (Fauzi *et al.*, 2023). This development presents opportunities for MSMEs not only to enhance their competitiveness (Mundzir *et al.*, 2021), but also to contribute to social solutions through innovative digital-based products and services. With over 215 million internet users and a high rate of mobile phone ownership, the digital MSME market holds significant potential, although challenges in digital security remain a primary concern. Despite growing public digital literacy, surveys indicate that digital security remains the weakest aspect, with an index score of only 3.12 on a scale of 5. This poses a significant risk of personal data breaches, which present a serious threat to users of digital business platforms, including MSME owners.

Personal data, which includes an individual's sensitive information (Rosadi, 2023), must be protected in accordance with applicable laws and regulations to safeguard every consumer's right to privacy. While digitalization enhances consumer convenience by enabling more efficient access to products and services, legal protection of personal data remains a crucial aspect in ensuring security and trust within the digital business ecosystem (Rizal, Rosadi and Taryana, 2024).

Law No. 20 of 2008, together with Government Regulation No. 17 of 2013, serves as the legal foundation for the regulation of MSMEs in Indonesia, aiming to protect and facilitate business operators in running their enterprises. The government continues to develop regulations to strengthen the MSME sector as a key driver of the national economy (Chandrawulan *et al.*, 2020). In its development, to address various legal challenges faced by MSME operators, the government enacted Law No. 11 of 2020 on Job Creation, which was later reinforced by Government Regulation No. 7 of 2021 on the facilitation, protection, and empowerment of MSMEs, as well as Government Regulation No. 8 of 2021, which regulates the minimum capital requirements for limited liability companies and the registration of micro and small enterprises.

The right to personal data protection is recognized under Article 28G(1) of the Constitution 1945, which affirms an individual's right to privacy, dignity, and security of person and property from all forms of threats. Various regulations in Indonesia govern personal data protection, including the Health Regulation, Banking Regulation, Telecommunications Regulation, Human Rights Regulation, Population Administration Regulation, and the Electronic Information and Transactions Regulation. Technological advancements and societal needs have driven the enactment of PDP Regulation as a measure to strengthen existing regulations. The PDP regulation aims to establish rights and obligations in personal data management, both domestically and internationally, covering individuals and legal entities, including the public and private sectors (Rosadi. and Pratama, 2018). With an approach aligned with international standards, this regulation is expected to enhance personal data protection and contribute to order and societal progress in the digital era (Sugeng, 2020).

The existence of various legal provisions governing personal data protection in Indonesia does not eliminate the risk of data breaches. In practice, numerous data leakage incidents continue to occur. Personal data breaches in Indonesia, such as the BPJS Ketenagakerjaan case, where 18.5 million user records were sold on the dark web (Argiansyah and Prawira, 2024), and the Bank

Syariah Indonesia breach, which resulted in the loss of 1.5 terabytes of data due to a LockBit ransomware attack (RDS, no date), demonstrate that even large entities with advanced security systems remain vulnerable to cyber threats. The 2023 passport data breach affecting 34 million Indonesian citizens, allegedly linked to the hacker Bjorka, further underscores that personal data protection remains suboptimal, despite the presence of strict regulations. This situation serves as a warning to all stakeholders, including MSMEs, which often face technological and budget constraints, to enhance data protection systems and mitigate similar risks.

In the context of MSME regulation in the digital transformation era, consumer personal data protection continues to face significant challenges, particularly in the implementation of adequate security standards in the user registration process. Although Indonesia has enacted regulations such as the PDP regulation, data breaches remain frequent due to weak enforcement and low awareness among MSME operators regarding the importance of data protection. In contrast, countries like Malaysia have adopted stricter and more systematic regulations, such as the Personal Data Protection Act (PDPA), which mandates more secure data management mechanisms. This regulatory gap highlights that, despite the existence of data protection laws in Indonesia, their effectiveness in safeguarding consumer personal data remains suboptimal. Therefore, this study aims to analyze how user registration strategies can be utilized to strengthen consumer personal data protection in digital MSME businesses, by comparing Malaysia's regulatory practices as a reference for policy improvement in Indonesia.

Research Method and Design

This article uses a normative juridical research type, conducted by examining literature or secondary data (Qamar *et al.*, 2017). This article aims to examine, analyze, and recommend the implementation of a registration system for MSMEs that manage large amounts of data to enhance compliance, transparency, and digital business security in Indonesia. The approach used includes the statute approach (Ariawan, 2013), which examines personal data protection regulations in Indonesia and Malaysia. The conceptual approach (Tan, 2021), analyzes legal concepts and theories on personal data protection, while the comparative law approach (Juliardi *et al.*, 2023), aims to identify the implementation practices of Data User Registration as a strategy to strengthen consumer personal data protection in digital MSME businesses in Indonesia. The data used consists of secondary data, which includes primary legal materials (legislation), secondary legal materials (books, scientific journals, and previous research), and tertiary legal materials (legal dictionaries and encyclopedias) (Ali, 2021). The data collection technique is carried out through document or literature studies (Efendi, Ibrahim and Rijadi, 2016), and observations on the implementation of data protection policies. The collected data is analyzed qualitatively using a descriptive-analytical method to interpret and relate various legal provisions and compare them with the system in Malaysia.

Results

Regulation of MSMEs through Personal Data Protection in Indonesia

Personal data protection is a fundamental human right and an integral part of individual self-protection; therefore, it requires a legal framework to ensure security over personal data based on the Constitution 1945. The current legislative framework for personal data regulation is governed by the Personal Data Protection Regulation to enhance the effectiveness of personal

data protection implementation. As the legal basic for personal data protection in Indonesia, the PDP Regulation provides the following regulations:

1) Types of Personal Data

Types of Personal Data are regulated under Article 3 of the PDP Regulation. Personal data is categorized into general personal data and specific personal data. General personal data includes full name, gender, nationality, religion, and/or other personal data that, when combined, can identify an individual. Specific personal data includes health and medical information, biometric data, genetic data, sexual life or orientation, political views, criminal records, child data, personal financial data, and/or other data as stipulated by applicable laws and regulations.

2) Rights of Personal Data Owners

The rights of personal data owners are stipulated in Chapter III, covering Articles 4 to 16 of the PDP regulation. These rights include, but are not limited to: The right to request information regarding the identity, legal basis, purpose of the request and use of personal data, and the accountability of the party requesting the data. The right to terminate processing, delete, and/or destroy their personal data. The right to withdraw consent previously given to the data controller for processing their personal data. The right to claim compensation for any personal data breach, in accordance with the applicable laws and regulations.

3) Processing of Personal Data

The processing of personal data is regulated in detail under a separate chapter, namely Chapter IV, which consists of six articles, from Article 17 to Article 22. The provisions on personal data processing are broad in scope, covering the methods of processing, the principles governing such processing, its purposes, ethical considerations, protections for personal data subjects, and the accompanying legal provisions.

4) Obligations of Data Controllers and Personal Data Processors

Personal Data Controllers and Processors include individuals, public entities, and organizations/institutions. They are required to provide information regarding the legality of personal data processing, the purpose of processing, the types and relevance of personal data to be processed, among other aspects, and must present evidence of consent granted by the data subject. Given the high potential for moral hazard that may affect data subjects due to actions taken by personal data controllers and processors, the regulations governing their obligations in personal data processing are extensive and comprehensive, covering 28 specific articles from Article 23 to Article 50. These regulations also include provisions on personal data transfers and administrative sanctions.

5) The prohibition on the use of personal data

This point includes prohibitions for parties who collect personal data that does not belong to them, install and/or operate visual data processing or processing tools that are not their own for personal gain, resulting in harm to the personal data owner.

6) The establishment of a code of conduct for personal data controllers.

This point relates to business actor associations in establishing a code of conduct for personal data controllers, taking into account the purpose of personal data processing, personal data protection principles, and the interests of personal data owners.

7) Dispute resolution and legal proceedings.

Article 56 regulates that personal data protection disputes are resolved through arbitration, court proceedings, or other alternative dispute resolution mechanisms.

8) International cooperation.

Regarding international cooperation in personal data protection, it is regulated in Article 57. International cooperation is carried out by the government with other national governments or international organizations in accordance with the provisions of laws and regulations and the principles of international law.

9) The role of the government and society

The government plays a role in implementing personal data protection, which is carried out by the minister. Society can participate, either directly or indirectly, in supporting the implementation of personal data protection.

10) Criminal provisions.

These provisions set out the legal consequences for violations of personal data protection regulations, including a maximum imprisonment of 7 years and a fine of up to IDR 70 billion.

Based on the provisions of Indonesia's Personal Data Protection Regulation mentioned above, this law does not explicitly require the registration of user data (User Registration Data) as implemented in Malaysia. The PDP regulation emphasizes the principles of personal data protection, including data subject rights, obligations of data controllers and processors, as well as supervision mechanisms and sanctions. In the context of digital MSMEs, the PDP regulation stipulates that business operators must obtain consent from data owners before collecting, using, or distributing personal data. However, there is no specific provision requiring MSMEs or digital platforms to register user data with a particular authority. Although there is no mandatory registration requirement, the PDP regulation still obliges data controllers to ensure the security and integrity of user data. This includes implementing security standards, mitigating the risk of data breaches, and the obligation to report data breach incidents.

Regulation of MSMEs through Personal Data Protection in Malaysia.

Personal data protection in Malaysia is governed by the Personal Data Protection Act 2010 (Malaysia PDP Act) and several supplementary regulations. The Malaysia PDP Act is intended to protect personal data by requiring data users to comply with specific obligations and granting certain rights to data subjects regarding their personal data. Before 2010, personal data regulation was largely governed by industry-specific laws. Industry-specific data protection laws applied to sectors such as banking and finance, healthcare, and telecommunications, among others. In May 2010, the Malaysia PDP Act was passed by the Malaysian Parliament and received Royal Assent in June 2010. The Act came into effect on November 15, 2013, with a three-month grace period ending on February 14, 2014 (Roslan *et al.*, 2022).

Along with the enforcement of the Malaysia PDP Act on November 15, 2013, five additional regulations were enacted to support its implementation, covering the appointment of the Commissioner, registration of data users, and applicable fees (Chesterman, 2012). Some of these regulations were later updated with additional regulations, namely: (1) the Personal Data Protection Regulations 2013; (2) the Personal Data Protection (Class of Data Users) Order 2013; (3) the Personal Data Protection (Registration of Data User) Regulations 2013; (4) the Personal Data Protection (Fees) Regulations 2013; (5) the Personal Data Protection (Compounding of Offences) Regulations 2016; (6) the Personal Data Protection (Class of Data Users) (Amendment) Order 2016; (7) the Personal Data Protection (Appeal Tribunal) Regulations 2021. In addition, the Commissioner issued the Personal Data Protection Standard 2015, which has been in effect since December 23, 2015, as the minimum standard for security, storage, and data integrity for all data users in commercial transactions (Sureani *et al.*, 2021). To ensure compliance in specific sectors such as communications, finance, insurance, hospitality, and others, data user forums were established to develop their respective codes of practice in accordance with the Commissioner's directives.

To date, six codes of practice have been registered by the Commissioner, namely: the Code of Practice for the Banking and Financial Sector 2017, the Personal Data Protection Code of Practice for the Utilities Sector (Electricity) 2017, the Code of Practice on Personal Data Protection for the Insurance and Takaful Industries in Malaysia 2017, the Personal Data Protection Code of Practice for the Communications Sector 2017, the Personal Data Protection Code of Practice for Private Hospitals in the Healthcare Industry 2022, the Personal Data Protection Code of Practice for the Utilities Sector (Water) 2022, dan the General Code of Practice of Personal Data Protection.

The Malaysia PDP Act applies to any individual or entity that processes or controls personal data, covering a wide scope of processing activities, including use, disclosure, collection, recording, and storage. Only individuals are recognized as data subjects under this law. While data processors acting on behalf of data users are not directly bound by the Act, data users are required to ensure their compliance. The Malaysia PDP Act does not apply to data processed outside Malaysia, except when it is further processed in Malaysia. Additionally, it does not apply to foreign data users, unless they use equipment located in Malaysia, except for transit purposes (Sholehuddin *et al.*, 2024). The Malaysian government, state governments, and data related to credit reporting businesses regulated under the Credit Reporting Agencies Act 2010 are also exempt from the provisions of this Act.

Data users are required to comply with the principles of personal data protection (Sudarwanto and Kharisma, 2022). The general principle of personal data processing requires that data be processed only for legitimate and relevant purposes, not excessively, and obtained with explicit consent through an opt-in method. Data users are responsible for proving that consent is properly recorded and stored. Consent requirements must be presented clearly and separately, while for data subjects under 18 years old, consent must be obtained from a parent or guardian (Cieh, 2013).

The principle of notice and choice requires data users to inform data subjects in writing, in both Malay and English, about data processing, including its purpose, source, access rights, third-party recipients, and options for restriction (Hassan, 2012). The notice must be provided at the time of data collection or before further use, in a clear and easily accessible manner, with flexibility for

additional languages if required. The principle of disclosure prohibits data users from disclosing personal data except for the purposes that have been informed, unless with the data subject's consent or for specific legal reasons (Ho, Dehghantanha and Shanmugam, 2010). Disclosure is permitted for crime prevention, legal obligations, public interest, or if the data user has a legal right. Additionally, data users must maintain a record of third-party disclosures for inspection by the Commissioner. The principle of security requires data users to implement protective measures to prevent loss, misuse, alteration, unauthorized access, or destruction of personal data. Under Malaysia's PDPA, factors to be considered include the nature of the data, storage location, security measures, reliability of personnel, and the security of data transfers (Sarabdeen and Ishak, 2024).

The principle of retention requires that personal data must not be kept longer than necessary and must be permanently destroyed or deleted when no longer needed. The 2015 Standards mandate that data users comply with relevant regulations before disposing of data, retain data only if required by law, record data disposal, discard collection forms within 14 days unless they hold legislative value, review and delete unnecessary data, establish a 24-month disposal schedule for inactive data, and prohibit storage on removable media without written management approval (Sureani *et al.*, 2021). The principle of data integrity requires data users to ensure that personal data is accurate, complete, not misleading, and continuously updated in accordance with the purpose of processing (Ong, 2012).

The Personal Data Protection Authority in Malaysia is the Personal Data Protection Commissioner (PDPC). The Personal Data Protection Commissioner is an entity under the Ministry of Communications and Digital (MCD). This authority was officially launched by the Minister in Kuala Lumpur on February 12, 2012 (Chan, 2024). The primary responsibility of the Personal Data Protection Commissioner (PDPC) is to enforce and regulate the Malaysia's PDPA, focusing on the processing of personal data in commercial transactions and preventing the misuse of personal data. In enforcing Malaysia's PDPA, the Commissioner is also mandated to register all categories of data users as specified by the regulation (Cheryl and Ng, 2022). The Commissioner has the authority to conduct inspections of data protection systems under Malaysia's PDPA. Other powers include, among others, the authority to appoint data user forums, issue and register codes of practice, conduct investigations upon receiving complaints, issue enforcement notices, and authorize officers to take enforcement actions.

The Malaysia's PDPA grants the following rights to data subjects:

1) Right to access personal data;
2) Right to request data users to correct personal data;
3) Right to withdraw consent for the processing of personal data;
4) Right to prevent processing that may cause harm or distress; and
5) Right to prevent processing for direct marketing purposes (Baskaran *et al.*, 2020).

The Malaysia's PDPA grants data subjects the right to request the cessation of their personal data processing for direct marketing by submitting a written notice to the data user (Putra, 2022). If this request is not complied with, the data subject may file a complaint with the Commissioner. Failure by the data user to comply with the Commissioner's order may result in a fine of up to MYR 200,000, imprisonment of up to two years, or both. Since January 11, 2015, complaints

related to data misuse can be submitted online through the Commissioner's website for further investigation (Kamaruddin *et al.*, 2021).

Malaysia's Personal Data Protection Act (PDPA) prohibits the transfer of personal data outside Malaysia, except when the transfer is made to a country specified and recorded in the Official Gazette by the Minister. Currently, no countries have been officially designated. Despite the general prohibition, the PDPA provides several exceptions, such as: if the data subject has given consent for the transfer. If the transfer is necessary for the performance of a contract between the parties. If there is uncertainty regarding whether a data transfer exception applies, a prudent approach would be to obtain the data subject's consent before transferring data outside Malaysia. Regarding outsourcing, data users are not permitted to share personal data with third parties unless the individual's consent has been obtained.

Malaysia's PDPA does not mandate the appointment of a Data Protection Officer (DPO). However, the data user registration application form requires the designation of a "compliance officer", who is identified as the individual responsible for overseeing the implementation of the PDPA within the data user's organization.

Currently, Malaysia's PDPA does not regulate data breach notification. However, the authorities have issued Public Consultation Paper 1/2018 on the Implementation of Data Breach Notification, which aims to introduce a data breach notification regime. Under this proposal, data users would be required to notify both regulators and affected individuals in the event of a data breach. The consultation paper outlines several key requirements, including: notifying the Commissioner within 72 hours of becoming aware of a data breach, providing details of the compromised data, outlining actions taken or planned to mitigate risks to the affected data, providing information on notifications made to impacted individuals, detailing the organization's data protection training programs. This proposal seeks to enhance accountability and transparency in handling data breaches within Malaysia (Haron, 2023). However, the consultation paper has not yet been enacted into law. While data breach notification is not a mandatory requirement under Malaysia's PDPA, data users may voluntarily notify the Commissioner online here. The required information includes details of the data user and the person submitting the notification, description of the data breach, mitigation and recovery measures taken, notifications sent to other parties, such as regulators, law enforcement agencies, affected individuals, data processors, or foreign data protection authorities (Teoh *et al.*, 2019).

If the processing of personal data is carried out by a data processor on behalf of a data user, the Malaysian Personal Data Protection Act requires, for the purpose of protecting personal data from loss, misuse, modification, unauthorized or accidental access, disclosure, alteration, or destruction, that the data user ensures the data processor:

1) Provides sufficient guarantees regarding the technical and organizational security measures governing the processing to be carried out; and

2) Takes reasonable steps to ensure compliance with those measures.

The security principle requires data users to establish a contract with data processors regarding any data processing activities (Low, 2021).

Failure to comply with the provisions of Malaysia's PDPA may be considered a criminal offense. Violations of any of the seven personal data protection principles can result in a fine of up to

MYR 300,000 (approximately $63,550) and/or up to two years of imprisonment. The unlawful collection, disclosure, and sale of personal data may be subject to a fine of up to MYR 500,000 (approximately $105,930) and/or up to three years of imprisonment. If a legal entity is found guilty of an offense, its officers are deemed to have committed the offense personally. The offenses specified so far relate to specific violations under the Malaysia PDPA, the 2013 Regulations, and the Registration Regulations (Pour, 2025). To meet registration requirements, digital MSMEs operating in mandatory sectors must submit their registration within three months of commencing operations. In cases of delays, valid reasons may be accepted(Cahya *et al.*, 2025).

Once registered, digital MSMEs are responsible for ensuring compliance with personal data protection principles, including security, integrity, and data retention. Referring to the Personal Data Protection Standard 2015, businesses are required to implement adequate security systems, such as customer data encryption, access restrictions to sensitive information (Vachkova *et al.*, 2023). The retention principle also requires MSMEs to delete or destroy customers' personal data once it is no longer needed for processing. This measure aims to prevent misuse or data breaches (Kanojia and Zahra, 2025). These measures not only protect consumers but also help MSMEs build a good reputation in the digital business sector.

For digital MSMEs that fail to comply with registration requirements or fail to protect customers' personal data, the Malaysia PDPA imposes severe penalties (Ismail *et al.*, 2023). If a digital MSME fails to register as a data user, it may face a fine of up to MYR 500,000 (approximately $106,000) or imprisonment for up to two years. Additionally, in cases of data breaches or misuse, businesses that negligently fail to implement protection standards may be subject to a fine of up to MYR 300,000 or imprisonment for up to one year, as stipulated in Section 5 of the Malaysia PDPA. These provisions highlight the Malaysian government's commitment to ensuring personal data protection in the digital era.

The implementation of data user registration regulations for digital MSMEs has a significant impact on the growth of Malaysia’s digital business ecosystem. These regulations help enhance consumer trust, leading to greater customer loyalty and more stable business growth. The Malaysian government continues to provide support in the form of technical guidance, subsidies, or incentives to help MSMEs adapt to regulations without hindering innovation or digital business expansion. The ultimate goal is for digital MSMEs in Malaysia to operate within a safer, fairer, and more transparent ecosystem.

The Importance of Data User Registration as a Strategy to Strengthen Consumer Personal Data Protection in Digital MSME Businesses

In the digital era, consumer personal data protection has become a crucial aspect of business sustainability, including for digital MSMEs that increasingly rely on technology in their operations. In Malaysia, the mandatory data user registration system under the Personal Data Protection (Registration of Data User) Regulations 2013 serves as one of the key strategies to strengthen personal data security. Under this requirement, MSMEs that process customer data in commercial transactions must register with the Personal Data Protection Commissioner. This process ensures that business entities handling personal data are under supervision and adhere to established compliance standards, thereby minimizing the potential for data misuse or breaches (Othman *et al.*, 2021).

The implementation of this registration system provides benefits for both MSMEs and consumers (Kanojia and Zahra, 2025). From the MSME perspective, having a data user registration certificate enhances business credibility and builds customer trust in the use of their digital services (Butarbutar, 2020). Consumers will feel more secure when sharing their personal information with a legally registered business, knowing that the business is subject to strict regulations in data processing (Mat *et al.,* 2019). Additionally, this mechanism facilitates authorities in monitoring violations and imposing sanctions on businesses that neglect or misuse customer data.

In addition to being a form of legal compliance, data user registration also encourages MSMEs to be more disciplined in managing personal data (Chuah and Thurusamry, 2021). With the registration requirement in place, MSMEs are encouraged to implement stricter internal policies regarding data processing, such as encrypting customer information, restricting data access, and adopting appropriate retention policies. This regulation fosters a safer and more responsible digital business ecosystem, where MSMEs not only focus on business growth but also on protecting consumer rights. Over time, this system can reduce the number of personal data breaches and create a more transparent and accountable digital business environment. Through registration, the government can identify and map business sectors with high risks of data breaches and provide education or support to business operators to enhance their compliance with personal data protection standards. This makes data user registration an effective preventive measure in addressing the ever-evolving cybersecurity challenges.

Through Law No. 27 of 2022 on Personal Data Protection, Indonesia has adopted many data protection principles that align with international standards. In Indonesia’s Law No. 27 of 2022 on Personal Data Protection, there is no explicit obligation for business operators to register as data users, as stipulated in Malaysia’s Personal Data Protection (Registration of Data User) Regulations 2013 (Ramadhan, 2022). However, the Indonesian PDPR mandates that Personal Data Controllers ensure compliance with personal data protection principles in data processing activities. This means that although there is no administrative requirement such as data user registration, business operators still have the responsibility to safeguard the security and integrity of the personal data they manage.

Several articles in Indonesia's PDPR are relevant to the obligations of data controllers. Article 23 stipulates that Personal Data Controllers must ensure the accuracy, relevance, and security of the personal data they manage. Additionally, Article 35 requires Personal Data Controllers to implement technical and organizational measures to protect data from misuse, breaches, or unauthorized access. Sanctions for violations are outlined in Articles 51 and 57, which specify administrative and criminal penalties for data controllers who fail to meet the data protection standards established under the PDPR.

In Malaysia, data users in specific sectors are required to register with the Personal Data Protection Commissioner and obtain a registration certificate before processing personal data (Surtiwa and Gultom, 2021). This mechanism enables stricter oversight of data users' compliance with personal data protection standards. In contrast, Indonesia's PDPR places greater emphasis on the responsibilities of Personal Data Controllers, including ensuring data security, adhering to data protection principles, and being accountable for data breaches or misuse (Diniyya, 2020). In other words, although registration is not mandatory, entities managing personal data must still implement security and data protection standards. However, the absence of a data user

registration requirement, as enforced in Malaysia, creates a regulatory gap that needs to be addressed. With the increasing number of personal data breaches across various sectors, Indonesia could adopt Malaysia's system by implementing a data user registration mechanism for businesses processing large volumes of consumer data, such as e-commerce, fintech, and other digital services. This regulation would enhance oversight of digital MSMEs and ensure that every business operator understands their responsibility in protecting consumer data.

The implementation of data user registration would also encourage increased awareness and compliance among MSMEs regarding data protection standards. If this mechanism is adopted, the government can support MSMEs through educational programs, training, and incentives for businesses that meet compliance standards. Consequently, Indonesia would not only strengthen consumer personal data protection but also foster a more trustworthy and globally competitive digital business ecosystem. In practice, the government could introduce future implementing regulations to further govern oversight mechanisms, including the possibility of a registration system for certain data controllers, particularly in sectors that process large volumes of data, such as banking, e-commerce, and fintech. This initiative aims to enhance transparency and accountability in personal data processing.

Conclusion

The implementation of a data user registration system is an effective strategy for strengthening consumer personal data protection in digital MSME businesses. A comparative study between Indonesia and Malaysia shows that Malaysia has adopted a data user registration mechanism requiring businesses to register before processing personal data, enabling stricter oversight of compliance with data protection standards. Meanwhile, Indonesia, through its PDPR, places greater emphasis on the responsibility of data controllers without mandating registration, which may create a regulatory gap in monitoring business compliance. Given the rising number of data breaches in Indonesia, this article recommends implementing a registration mechanism for businesses that process large volumes of consumer data, such as e-commerce and fintech, to enhance transparency, accountability, and MSMEs awareness of personal data protection. With this policy, Indonesia can establish a safer, more trustworthy, and globally competitive digital business ecosystem.

Acknowledgements

We extend our deepest gratitude and appreciation to:

1. The Indonesia Endowment Fund for Education (*Lembaga Pengelola Dana Pendidikan*) of the Ministry of Finance of the Republic of Indonesia for sponsoring and funding the research and publication of this article.
2. The Doctoral Program in Law at Universitas Padjadjaran, Bandung, as the institution where the author is employed and pursuing doctoral studies in the field of law.
3. The Faculty of Law, Universitas Pattimura, Ambon, where the author serves as a lecturer.
4. The Ministry of Cooperatives and SMEs of the Republic of Indonesia and the Ministry of Communication and Informatics of the Republic of Indonesia for providing data and information to support this research article.

5. The Provincial Government of Maluku and the Provincial Government of West Java, particularly the Office of Cooperatives and Small Enterprises and the Office of Communication and Informatics, for their willingness to provide data and information to enhance this research.

References

Ali, Z. (2021) Metode penelitian hukum. Sinar Grafika.

Argiansyah, H.Y. and Prawira, M.R.Y. (2024) 'Perlindungan Hukum Hak Atas Privasi Dan Perlindungan Data Pribadi Berdasarkan Perspektif Hak Asasi Manusia', Jurnal Hukum Pelita, 5(1), pp. 61–75. https://doi.org/10.37366/jh.v5i1.3946.

Ariawan, I.G.K. (2013) 'Metode Penelitian Hukum Normatif', Kertha Widya, 1(1).

Baskaran, H. et al. (2020) 'Blockchain and the personal data protection act 2010 (PDPA) in Malaysia', in 2020 8th International Conference on Information Technology and Multimedia (ICIMU). IEEE, pp. 189–193. 10.1109/ICIMU49871.2020.9243493.

Butarbutar, R. (2020) 'Personal data protection in P2P lending: What Indonesia should learn from Malaysia?', Pertanika Journal of Social Sciences and Humanities, 28(3), pp. 2295–2307. http://www.pertanika.upm.edu.my/pjssh/browse/regular-issue?article=JSSH-5415-2019.

Cahya, H.N. et al. (2025) Marketing and MSMEs dynamics in Indonesia and Malaysia: strategies, challenges, and cultural influences. Penerbit P4I.

Chan, M. (2024) 'Malaysia: Digital payments, data regulations, and ai as most promising areas for digital economy collaboration', in The ASEAN Digital Economy. Routledge, pp. 76–96.

Chandrawulan, A.A. et al. (2020) 'Potensi UMKM Di Pangandaran Dalam Menghadapi Masyarakat Ekonomi Asean', Jurnal Kumawula, 3(2), pp. 367–373. https://doi.org/10.24198/kumawula.v3i2.

Cheryl, B.-K. and Ng, B.-K. (2022) 'Protecting the unprotected consumer data in internet of things: Current scenario of data governance in Malaysia', Sustainability, 14(16), p. 9893. https://doi.org/10.3390/su14169893.

Chesterman, S. (2012) 'After Privacy: The Rise of Facebook, The Fall of Wikileaks, And Singapore's Personal Data Protection Act 2012', Sing. J. Legal Stud., p. 391. https://heinonline.org/HOL/LandingPage?handle=hein.journals/sjls2012&div=28&id=&page=.

Chuah, M.H. and Thurusamry, R. (2021) 'Challenges of big data adoption in Malaysia SMEs based on Lessig's modalities: A systematic review', Cogent Business & Management, 8(1), p. 1968191. https://doi.org/10.1080/23311975.2021.1968191.

Cieh, E.L.Y. (2013) 'Personal data protection and privacy law in Malaysia', Beyond Data Protection: Strategic Case Studies and Practical Guidance, pp. 5–29. https://doi.org/10.1007/978-3-642-33081-0_2.

Cihuy, P.G. (2019) Mencari Peluang di REVOLUSI INDUSTRI 4.0 Untuk Melalui Era Disrupsi 4.0: Queen Publisher. Queency Publisher.

Deni, A. (2023) Manajemen Strategi di Era Industri 4.0. Cendikia Mulia Mandiri.

Dewa, D.D. (2022) 'Masa Depan Penataan Ruang di Indonesia dalam Masa Transisi Menuju Masyarakat 5.0', TATALOKA, 24(1), pp. 62–73. https://doi.org/10.14710/tataloka.24.1.62-73.

Diniyya, A.. (2020) 'Financial technology regulation in Malaysia and Indonesia: a comparative study', Ihtifaz: Journal of Islamic Economics, Finance, and Banking, 3(2), pp. 67–87. https://doi.org/10.12928/ijiefb.v3i2.2703.

Efendi, J., Ibrahim, J. and Rijadi, P. (2016) 'Metode Penelitian Hukum: Normatif dan Empiris'.

Ekowati, D. et al. (2023) Rencana Bisnis 4.0. Cendikia Mulia Mandiri.

Fauzi, A.A. et al. (2023) Pemanfaatan Teknologi Informasi di Berbagai Sektor Pada Masa Society 5.0. PT. Sonpedia Publishing Indonesia.

Fonna, N. (2019) Pengembangan revolusi industri 4.0 dalam berbagai bidang. Guepedia.
Haqqi, H. and Wijayati, H. (2019) Revolusi industri 4.0 di tengah society 5.0: sebuah integrasi ruang, terobosan teknologi, dan transformasi kehidupan di era disruptif. Anak Hebat Indonesia.
Haron, M.H. (2023) 'Legal Review on CPTPP and its Implication on Bumiputera's Policies in Malaysia Government Procurement', Journal of Central Banking Law and Institutions, 2(3), pp. 543–556. https://doi.org/10.21098/jcli.v2i3.179.
Hassan, K.H. (2012) 'Personal data protection in employment: New legal challenges for Malaysia', Computer Law & Security Review, 28(6), pp. 696–703. https://doi.org/10.1016/j.clsr.2012.07.006.
Ho, V., Dehghantanha, A. and Shanmugam, K. (2010) 'A guideline to enforce data protection and privacy digital laws in Malaysia', in 2010 Second International Conference on Computer Research and Development. IEEE, pp. 3–6. 10.1109/ICCRD.2010.92.
Ifadhila, I. et al. (2024) Pemasaran Digital di Era Society 5.0: Transformasi Bisnis di Dunia Digital. PT. Sonpedia Publishing Indonesia.
Ismail, S. et al. (2023) 'Digitalisation of micro-enterprises: Data acquisition for sustainability governance', in AIP Conference Proceedings. AIP Publishing.
Juliardi, B. et al. (2023) Metode penelitian hukum. CV. Gita Lentera.
Juwita, D. and Handayani, A.N. (2022) 'Peluang dan Tantangan Digitalisasi UMKM Terhadap Pelaku Ekonomi di Era Society 5.0', Jurnal Inovasi Teknologi Dan Edukasi Teknik, 2(5), pp. 249–255. https://doi.org/10.17977/um068v2i52022p249-255.
Kamaruddin, S. et al. (2021) 'The quandary in data protection and rights to privacy of AI technology adoption in Malaysia', in 2021 Innovations in Power and Advanced Computing Technologies (i-PACT). IEEE, pp. 1–5. 10.1109/i-PACT52855.2021.9696803.
Kanojia, S. and 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. IGI Global Scientific Publishing, pp. 443–462. DOI: 10.4018/979-8-3693-6740-7.ch018.
Kementerian Koperasi dan UKM (2023) UMKM Dalam Angka Tahun 2023.
Low, C.C. (2021) 'Digitalization of migration management in Malaysia: Privatization and the role of immigration service providers', Journal of International Migration and Integration, 22(4), pp. 1599–1627. https://doi.org/10.1007/s12134-021-00809-1.
Manan, B. (1995) Pertumbuhan dan Perkembangan Konstitusi Suatu Negara. Bandung: Mandar Maju.
Mat, B. et al. (2019) 'Cybersecurity and digital economy in Malaysia: Trusted law for customer and enterprise protection', International Journal of Innovative Technology and Exploring Engineering, 8(3), pp. 214–220. https://www.ijitee.org/wp-content/uploads/papers/v8i8s3/H10610688S319.pdf.
Mundzir, A. et al. (2021) Peningkatan Ekonomi Masyarakat menuju Era Society 5.0 Ditengah Pandemi Covid-19. Penerbit Insania.
Ong, R. (2012) 'Data protection in Malaysia and Hong Kong: One step forward, two steps back?', computer law & security review, 28(4), pp. 429–437. https://doi.org/10.1016/j.clsr.2012.05.002.
Othman, I.W. et al. (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), pp. 124–143. https://www.researchgate.net/publication/356718178_Driving_The_Development_Of_SMEs'_Entrepreneurs_In_The_Era_Of_Digitalisation_From_The_Dynamic_Perspective_Of_Law_Enforcement_In_Malaysia.
Pour, H.N. (2025) 'Data Protection Challenges In Smart Cities: An Examination Of The Malaysian Legal Framework', UUM Journal of Legal Studies, 16(1), pp. 115–129. https://doi.org/10.32890/uumjls2025.16.1.7.

Putra, Y. (2022) 'Comparison of personal data protection laws using narrative policy framework between indonesia, malaysia, and Japan', Negrei Academic Journal of Law and Governance, 2(2), p. 99. 10.29240/negrei.v2i2.5527.

Qamar, N. et al. (2017) Metode Penelitian Hukum (Legal Research Methods). CV. Social Politic Genius (SIGn).

Ramadhan, K.R. (2022) 'The Challenges of Personal Data Protection Policy in Indonesia: Lesson learned from the European Union, Singapore, and Malaysia', Technium Soc. Sci. J, 36, p. 18. https://doi.org/10.47577/tssj.v36i1.7442.

RDS (no date) Deret Insiden Kebocoran DATA wno 2023, BPJS Hingga Dukcapil.

Rizal, M., Rosadi, S.D. and Taryana, A. (2024) 'Legal Framework for consumer Data Protection For Digital Business SMES in Indonesia', Journal of Law and Sustainable Development, 12(1), pp. e2809–e2809. https://doi.org/10.55908/sdgs.v12i1.2809.

Rosadi., S.D. and Pratama, G.G. (2018) 'Perlindungan Privasi dan Data Pribadi dalam Era Ekonomi Digital Di Indonesia', Veritas et Justitia, 4(1), pp. 88–110. https://doi.org/10.25123/vej.v4i1.2916.

Rosadi, S.D. (2023) Pembahasan UU Pelindungan Data Pribadi (UU RI Nomor 27 Tahun 2021). Jakarta: Sinar Grafika.

Roslan, A.K. et al. (2022) 'Legal Protection of E-Consumers in Malaysia', International Journal of Law, Government and Communication, 7(29), pp. 223–241. 10.35631/IJLGC.729016.

Sarabdeen, J. and Ishak, M.M.M. (2024) 'A comparative analysis: health data protection laws in Malaysia, Saudi Arabia and EU General Data Protection Regulation (GDPR)', International Journal of Law and Management, 67(1), pp. 99–119. https://doi.org/10.1108/IJLMA-01-2024-0025.

Savitri, A. (2019) 'Mengubah Tantangan Menjadi Peluang di Era Disrupsi 4.0', Jogjakarta: Genesis.

Sholehuddin, N. et al. (2024) 'A Comparative Legal Analysis on Personal Data Protection Laws in Selected ASEAN Countries: Analisis Perundangan Perbandingan Undang-undang Perlindungan Data Peribadi di Negara-negara ASEAN', Journal of Muwafaqat, 7(1), pp. 23–38. https://doi.org/10.53840/muwafaqat.v7i1.166.

Soewardi, H. (1989) Koperasi: Suatu Kumpulan Makalah. Bandung: IKOPIN.

Srikalimah, S. et al. (2020) 'Do creativity and intellectual capital matter for SMEs sustainability? The role of competitive advantage', The Journal of Asian Finance, Economics and Business, 7(12), pp. 397–408. 10.13106/jafeb.2020.vol7.no12.397.

Sudarwanto, A.S. and Kharisma, D.B.B. (2022) 'Comparative study of personal data protection regulations in Indonesia, Hong Kong and Malaysia', Journal of Financial Crime, 29(4), pp. 1443–1457. 10.1108/JFC-09-2021-0193.

Sugeng (2020) Hukum Telematika Indonesia. Jakarta: Kencana.

Sureani, N.B.N. et al. (2021) 'The Adequacy of Data Protection Laws in Protecting Personal Data in Malaysia', Malaysian Journal of Social Sciences and Humanities (MJSSH), 6(10), pp. 488–495. https://doi.org/10.47405/mjssh.v6i10.1087.

Surtiwa, S.S. and Gultom, C.J. (2021) 'ASEAN for Data Protection', in Asia-Pacific Research in Social Sciences and Humanities Universitas Indonesia Conference (APRISH 2019). Atlantis Press, pp. 720–726. 10.2991/assehr.k.210531.090.

Tan, D. (2021) 'Metode penelitian hukum: Mengupas dan mengulas metodologi dalam menyelenggarakan penelitian hukum', Nusantara: Jurnal Ilmu Pengetahuan Sosial, 8(8), pp. 2463–2478. DOI : 10.31604/jips.v8i8.2021.2463-2478.

Teoh, M.T.T. et al. (2019) 'The Regulatory Framework of Digital Currencies in Malaysia: A Conceptual Paper', European Proceedings of Social and Behavioural Sciences, 89, pp. 258–269. 10.15405/epsbs.2020.10.02.24.

Vachkova, M. et al. (2023) 'Big data and predictive analytics and Malaysian micro-, small and medium businesses', SN Business & Economics, 3(8). 10.1007/s43546-023-00528-y.

Wibowo, A. (2023) Revolusi 4.0 dan Society 5.0. Semarang: Yayasan Prima Agus Teknik.

Yahanan, A., Febrian, F. and Rahim, R.A. (2017) 'The Protection of Consumer Rights for Aviation Safety and Security in Indonesia and Malaysia', Sriwijaya Law Review, 1, pp. 27–43. http://dx.doi.org/10.28946/slrev.Vol1.Iss1.7.pp027-043.