

Legal Protection of MSME Data in Government Digitalization Programs as an Instrument for Enhancing National Economic Competitiveness

Ahmad Gautsul Anam¹ Panji Rizki Kurniawan² Irwan W³ Muhammad Budi Utama⁴
Fahrul Hudatil Atkiyan⁵

Akademi Bisnis Lombok¹ Akademi Bisnis Lombok² Akademi Bisnis Lombok³
Akademi Bisnis Lombok⁴ Akademi Bisnis Lombok⁵

Correspondence: gautsulanam98@gmail.com

Article Info:

Received: 02/06/2026

Revised: 15/07/2026

Accepted: 01/08/2026

Abstract

The digital transformation agenda promoted by the Indonesian government through various digitalization programs for Micro, Small, and Medium Enterprises (MSMEs) has generated a substantial accumulation of business-related data, encompassing identity information, transaction records, and financing histories. This development raises a fundamental legal question concerning the extent to which the national legal framework is capable of safeguarding such data against misuse and data breaches. This article aims to examine the scope and adequacy of legal protection afforded to MSME data within government-led digitalization programs and to assess its relevance to enhancing national economic competitiveness. The study employs a normative juridical method using both statutory and conceptual approaches, examining Law Number 27 of 2022 on Personal Data Protection in conjunction with sectoral regulations governing MSMEs and public data governance. The findings indicate that although the Personal Data Protection Law has established the foundational principles of data protection, its implementation within MSME digitalization programs continues to exhibit significant gaps. These include weak accountability mechanisms for data controllers within government institutions, limited legal literacy among MSME actors, and the absence of comprehensive integration of data protection principles into the National One Data policy framework. Therefore, strengthening implementing regulations, enhancing inter-agency oversight, and expanding legal education for MSME actors are essential to fostering digital trust, thereby contributing to the improvement of Indonesia's national economic competitiveness.

Keywords: Personal Data Protection; Micro, Small, and Medium Enterprises (MSMEs); Government Digitalization; Economic Competitiveness; Data Governance.

INTRODUCTION

The Government of Indonesia has actively promoted the acceleration of the digitalization of Micro, Small, and Medium Enterprises (MSMEs) as part of its broader strategy to enhance the sector's contribution to national economic development. Various initiatives have been implemented, including the expansion of the Quick Response Code Indonesian Standard (QRIS), which has been adopted by tens of millions of

MSME users, the integration of MSMEs into electronic commerce platforms through digital onboarding programs, and the establishment of an integrated business data system under the *One Data Indonesia* framework as mandated by Presidential Regulation Number 39 of 2019. In addition, numerous ministries and government agencies collect MSME-related data through business licensing systems, the distribution of People's Business Credit (*Kredit Usaha Rakyat*), fiscal incentive programs, and product certification schemes. Consequently, the government's digital ecosystem stores extensive datasets encompassing personal identification information, transaction records, financial histories, and business location data.

The accumulation of such large-scale datasets offers significant advantages, including greater efficiency in public service delivery and more evidence-based policymaking. Nevertheless, it also introduces new legal and governance challenges, particularly the risks of unauthorized access, data breaches, misuse of personal information, and secondary use of data beyond the purposes for which it was originally collected. These concerns are further exacerbated by the fact that many MSME actors possess only limited awareness of their rights concerning personal data protection, while some government institutions acting as data controllers have yet to fully implement the security standards and accountability mechanisms required under Law Number 27 of 2022 on Personal Data Protection.

Existing scholarship on personal data protection in Indonesia has predominantly focused on general contexts, including digital identity systems, financial services, and electronic commerce. Comparatively little attention has been devoted to examining the legal status and protection of MSME data within government-led digitalization programs and its relationship to the broader objective of strengthening national economic competitiveness. This gap is significant because the confidence of MSME actors in the security and lawful management of their personal data constitutes an essential prerequisite for sustainable digital adoption, which in turn supports the competitiveness of small enterprises in both domestic and international markets.

Against this background, this article addresses two principal research questions. First, what forms of legal protection are available for MSME data within government digitalization programs? Second, to what extent are these legal protections adequate to support the enhancement of Indonesia's national economic competitiveness? The novelty of this study lies in its integration of the legal framework governing personal data protection with the practical governance of data within government digitalization initiatives for MSMEs. Furthermore, the study situates personal data protection not merely as an issue of individual privacy rights but also as a strategic component of national economic policy and sustainable digital economic development.

RESEARCH METHOD

This study employs a normative juridical research method, in which positive legal norms constitute the primary object of analysis. The research adopts both a statutory approach and a conceptual approach. The statutory approach is utilized to examine Law Number 27 of 2022 on Personal Data Protection, Law Number 20 of 2008 on Micro, Small, and Medium Enterprises (MSMEs), and Presidential Regulation Number 39 of

2019 on *One Data Indonesia*, together with their relevant implementing regulations. The conceptual approach is applied to analyze the principles and theoretical foundations of personal data protection developed within legal scholarship, with the objective of assessing the extent to which the existing legal framework adequately addresses the data protection needs of MSMEs.

The legal materials employed in this study consist of primary, secondary, and tertiary legal sources. Primary legal materials include the statutory instruments referred to above. Secondary legal materials comprise scholarly journal articles, academic books, and reports issued by government institutions concerning personal data protection and the digitalization of MSMEs. Tertiary legal materials include legal dictionaries and glossaries of technical terminology. These legal materials were collected through library research by systematically identifying, reviewing, and selecting sources relevant to the research questions.

The legal materials were analyzed using a descriptive-qualitative method through systematic and teleological interpretation. Systematic interpretation was employed to examine personal data protection norms within the broader context of the Indonesian legal system, while teleological interpretation was used to ascertain the legislative objectives underlying the relevant statutory provisions. The results of these interpretative analyses were subsequently examined in relation to the governance of MSME data within government-led digitalization programs in order to evaluate the adequacy of the existing legal protection framework and its contribution to enhancing national economic competitiveness.

RESULTS

Legal Framework for Personal Data Protection of MSMEs

Law Number 27 of 2022 on Personal Data Protection constitutes the principal legal framework governing the processing of personal data in Indonesia, including the personal data of Micro, Small, and Medium Enterprises (MSMEs) operating as individually owned businesses. The Law establishes a set of fundamental principles that must be observed by data controllers, including the acquisition of valid consent from data subjects, the limitation of data processing to specified and legitimate purposes, the maintenance of data accuracy, and the obligation to ensure data security through appropriate technical and organizational measures. Accordingly, government institutions that collect MSME data for purposes such as business registration, financing distribution, and the provision of fiscal or non-fiscal incentives are legally recognized as data controllers and are therefore subject to these statutory obligations.

Beyond the Personal Data Protection Law, several sector-specific regulations also shape the governance of MSME data. Among these is Presidential Regulation Number 39 of 2019 on *One Data Indonesia*, which establishes the principles of data interoperability among government agencies, as well as various ministerial regulations that provide the legal basis for the implementation of Electronic-Based Government Systems (*Sistem Pemerintahan Berbasis Elektronik/SPBE*). Collectively, these regulatory instruments demonstrate that a legal framework for the protection of MSME personal data is already

in place. Nevertheless, the framework remains fragmented across multiple legal instruments that have yet to be fully harmonized and integrated, thereby limiting the consistent articulation and enforcement of data protection obligations across institutional sectors.

Patterns of Data Collection and Processing in Government-Led MSME Digitalization Programs

Government-led digitalization initiatives collect MSME data through a variety of digital platforms and administrative channels, including online business licensing registration systems, integrated MSME and cooperative databases developed in collaboration with national statistical agencies, program-based credit information systems for the distribution of People's Business Credit (Kredit Usaha Rakyat/KUR), MSME taxation databases, and QRIS-based digital payment ecosystems. Each of these channels is administered by different government institutions, resulting in identical data concerning an individual business owner being stored and processed independently by multiple data controllers.

While this decentralized data governance model substantially enhances the efficiency of evidence-based policymaking and public service delivery, it simultaneously expands the overall **risk surface** associated with personal data processing, particularly when one or more systems fail to implement adequate technical and organizational security safeguards. A significant finding of this study is the absence of a standardized auditing and oversight mechanism applicable to all government electronic systems involved in the processing of MSME data. This regulatory and institutional fragmentation has the potential to undermine the consistent implementation of personal data protection principles and to increase the likelihood of unauthorized access, data breaches, and misuse of personal information across interconnected governmental databases.

Gaps in the Legal Protection Framework

An examination of the prevailing legal framework and its practical implementation reveals at least three fundamental gaps in the protection of personal data within the context of MSME digitalization. First, not all government institutions responsible for processing MSME data have appointed designated officers or officials accountable for personal data protection, as mandated under Law Number 27 of 2022 on Personal Data Protection. This institutional deficiency weakens internal governance mechanisms and limits organizational accountability in ensuring compliance with statutory data protection obligations.

Second, although the **One Data Indonesia** policy promotes interoperability and data integration across government agencies, it does not explicitly require the incorporation of the **data protection by design** principle during the planning and development of electronic information systems. Consequently, system interoperability tends to prioritize administrative efficiency and data exchange without ensuring that privacy and personal data protection safeguards are embedded throughout the system development lifecycle.

Third, the level of legal literacy among MSME actors regarding their rights as personal data subjects remains relatively low. As a result, the consent mechanism—which should function as an informed, voluntary, and meaningful expression of the data subject's autonomy—frequently operates as a mere administrative formality rather than as a substantive safeguard for informational self-determination. This condition ultimately diminishes the effectiveness of consent as one of the foundational principles of personal data protection and reinforces the structural imbalance between data controllers and data subjects.

DISCUSSION

The findings of this study demonstrate that the protection of MSME personal data extends beyond the realm of individual privacy rights and constitutes a strategic issue closely linked to the enhancement of national economic competitiveness. Trust among MSME actors in the security and integrity of their personal data represents a fundamental prerequisite for the sustainable adoption of digital technologies. Where business owners perceive their personal data to be vulnerable to unauthorized access, misuse, or disclosure, they are less likely to participate fully in government-led digitalization initiatives. Consequently, the anticipated economic benefits of digital transformation—including broader access to financing, greater transactional efficiency, and expanded market opportunities—may not be fully realized.

When compared with internationally recognized data protection frameworks, particularly those emphasizing the principles of **accountability** and **data protection by design** adopted in numerous jurisdictions, Indonesia's legal framework has, in principle, incorporated comparable normative standards through Law Number 27 of 2022 on Personal Data Protection. Nevertheless, the operationalization of these principles within Electronic-Based Government Systems (Sistem Pemerintahan Berbasis Elektronik/SPBE) continues to require more comprehensive implementing regulations. In particular, greater regulatory specificity is needed regarding minimum cybersecurity and information security standards for systems processing MSME data, as well as institutional mechanisms for coordinated oversight across ministries and government agencies to ensure consistent compliance with personal data protection obligations.

From a public policy perspective, the limited level of legal literacy among MSME actors highlights the necessity of integrating personal data protection education into digitalization programs themselves, rather than confining educational initiatives solely to the technical operation of digital applications. Government authorities should ensure that every MSME registration, data collection, or digital transformation program is accompanied by clear, accessible, and comprehensible information concerning the purposes of data collection, the entities authorized to access the data, and the legal rights of business owners to request data correction, object to certain processing activities, and exercise other rights guaranteed under the Personal Data Protection Law. Such measures are fully consistent with the principle of **transparency**, which constitutes one of the foundational pillars of Indonesia's personal data protection regime.

This study is subject to several limitations. As a normative legal study, it does not incorporate empirical field data concerning the perceptions or experiences of MSME

actors regarding personal data protection. Accordingly, the conclusion that legal literacy among MSME actors remains relatively limited is derived from doctrinal analysis and the existing body of literature rather than from direct empirical measurement. Future research employing empirical methodologies is therefore recommended to validate and expand upon these findings, particularly by assessing MSME actors' awareness and understanding of their legal rights as data subjects within government digitalization programs.

Overall, strengthening the legal protection of MSME personal data should be regarded as an institutional investment that contributes to long-term economic competitiveness. A robust and trustworthy data protection framework is capable of fostering greater digital trust, thereby encouraging broader MSME participation in the digital economy, facilitating data-driven access to financial services, and ultimately enhancing the contribution of MSMEs to sustainable national economic development. This perspective underscores that effective personal data protection is not merely a legal compliance obligation but also a strategic enabler of inclusive digital transformation and resilient economic growth.

CONCLUSION

Indonesia has established a comprehensive legal framework for the protection of MSME personal data through **Law Number 27 of 2022 on Personal Data Protection**, complemented by sector-specific regulatory instruments such as the **One Data Indonesia** policy. Nevertheless, the implementation of this framework within government-led MSME digitalization programs continues to face several significant challenges. These include deficiencies in the accountability of government data controllers, the insufficient integration of personal data protection principles into data interoperability policies, and the relatively low level of legal literacy among MSME actors regarding their rights as personal data subjects.

This study demonstrates that strengthening the legal protection of MSME personal data carries both theoretical and practical significance. From an academic perspective, it broadens the discourse on personal data protection by situating it within the broader context of economic governance and digital transformation policies. From a practical standpoint, the findings provide a valuable reference for policymakers in formulating more detailed implementing regulations to enhance the effectiveness of Indonesia's personal data protection regime. Policy measures that merit consideration include the issuance of comprehensive technical guidelines on information security for all government electronic systems processing MSME data, the appointment of designated Data Protection Officers or equivalent officials within relevant government institutions, and the integration of legal awareness and personal data protection education into MSME digitalization initiatives. Such measures are expected to strengthen institutional accountability while fostering greater public trust in digital governance.

Finally, future research should adopt empirical approaches to examine directly the level of legal awareness, understanding, and lived experiences of MSME actors regarding the protection of their personal data within government digitalization programs. Empirical evidence of this nature would complement the normative findings of the present study

and contribute to the development of more evidence-based legal and policy reforms capable of supporting a secure, trustworthy, and inclusive digital economy.

REFERENCES

- Andika, F., Rasmuddin, & Hamzah, I. F. (2026). Perlindungan Hukum Terhadap Data Pribadi dalam Era Digital. *Unes Journal of Swara Justisia*, 9(4), 825–832. <https://doi.org/10.31933/ysc6n689>
- Badan Pusat Statistik & Kementerian Koperasi dan Usaha Kecil dan Menengah. (2023). *Pendataan Lengkap Koperasi, Usaha Mikro, Kecil, dan Menengah (PL-KUMKM)*. Badan Pusat Statistik.
- Darnela, L., & Rusdiana, E. (2025). Public Awareness and Legal Compliance with Indonesia's Personal Data Protection Law: An Empirical Study in the Digital Era. *Supremasi Hukum: Jurnal Kajian Ilmu Hukum*, 14(1), 2–28.
- Kementerian Komunikasi dan Digital Republik Indonesia. (2024). *Era Baru Perlindungan Data Pribadi*. <https://djkgpm.komdigi.go.id/berita/artikel/35/era-baru-perlindungan-data-pribadi>
- Lestari, E., & Rasji. (2024). Legal Study on Personal Data Protection Based on Indonesian Legislation. *Awang Long Law Review*, 6(2), 471–477. <https://doi.org/10.56301/awl.v6i2.1206>
- Palit, S. M. L., & Purba, T. L. D. (2025). Legal Perspective on Data Privacy Protection as a Human Right in Indonesia. *The Easta Journal Law and Human Rights*, 4(01), 24–32. <https://doi.org/10.58812/eslhr.v4i01.783>
- Republik Indonesia. (2008). *Undang-Undang Nomor 20 Tahun 2008 tentang Usaha Mikro, Kecil, dan Menengah*. Lembaran Negara Republik Indonesia.
- Republik Indonesia. (2019). *Peraturan Presiden Nomor 39 Tahun 2019 tentang Satu Data Indonesia*. Lembaran Negara Republik Indonesia.
- Republik Indonesia. (2022). *Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi*. Lembaran Negara Republik Indonesia. <https://peraturan.bpk.go.id/Details/229798/uu-no-27-tahun-2022>
- Rinjani, M. A., & Firmansyah, R. (2025). Hambatan Implementasi UU 27/2022 dan Strategi Penguatan Perlindungan Data Pribadi di Indonesia. *Jurnal Analisis Hukum*, 8(1), 70–83. <https://doi.org/10.38043/jah.v8i1.6793>