Legal Autonomous Web-based Governance (LAW)
Vol. 1, No. 1, June 2026, pp. 95∼108
E-ISSN: 3164-6794 | P-ISSN: 3164-6697, DOI: 10.68012

Legal Governance of Personal Data Protection in Indonesian Digital Business

Dwi Cahyono[1*], Denok Wahyudi Setyo Rahayu[2], Mungkap Mangapul Siahaan[3], John Edwards[4]
[1]Faculty of Economic and Business, University of Muhammadiyah Jember, Indonesia
[2]Fakultas Ekonomi Program Studi Manajemen, Universitas Islam Balitar, Indonesia
[3]Faculty of Teacher Training and Education, Universitas HKBP Nommensen Pematangsiantar, Indonesia
[4]Department of Law and Information Technology, Pandawan Incorporation, New Zealand
[1]dwicahyono@unmuhjember.ac.id, [2]denokwahyudisr@unisbablitar.ac.id, [3]mungkapsiahaan@gmail.com, [4]j.edwards@pandawan.ac.nz
***Corresponding Author**

Article Info

Article history:

Submission, March 12, 2026
Revised, May 25, 2026
Accepted, June 17, 2026
Published, June 25, 2026

Keywords:

Personal Data Protection
Digital Business
Data Governance
Legal Framework
Digital Ecosystem

ABSTRACT

This study examines the legal framework for personal data protection in Indonesia digital business ecosystem following the enactment of Law No. 27 of 2022 on Personal Data Protection. As a rapidly growing digital economy, Indonesia represents a transitional legal environment seeking to translate global privacy principles into enforceable domestic regulations, unlike jurisdictions with more established frameworks such as the GDPR. **This study aims** to analyze the legal architecture of Indonesia personal data protection regime and its implications for governance within the digital business sector. **Using a normative** legal research approach combined with regulatory analysis, this study examines Law No. 27 of 2022, its institutional enforcement mechanisms, and relevant regulations governing electronic systems and digital platforms, including the Electronic Information and Transactions Law. **The findings** reveal that Indonesia has incorporated key international data protection principles, including lawfulness, transparency, purpose limitation, and accountability. However, their implementation continues to face challenges related to regulatory coordination, supervisory authority, enforcement capacity, and compliance readiness among digital business actors. **The Indonesian experience** illustrates the complexity of harmonizing global data protection standards with domestic legal structures in emerging digital economies. Strengthening institutional enforcement, clarifying supervisory responsibilities, and improving regulatory coherence are therefore essential to ensuring effective personal data protection and supporting the sustainable growth of Indonesia digital ecosystem.

This is an open access article under the CC BY 4.0 license.

DOI: https://doi.org/10.68012/law.v1i1.113
This is an open access article under the CC BY license (https://creativecommons.org/licenses/by/4.0/)
©Authors retain all copyrights

1. INTRODUCTION

The rapid advancement of information and communication technology has transformed economic activities in Indonesia, leading to the expansion of digital business ecosystems such as e-commerce, fintech, social commerce, and platform-based services [1]. These platforms depend heavily on the collection, processing, and storage of personal data to provide personalized and data-driven services. As personal data increasingly becomes a strategic asset in digital business models, concerns regarding data breaches, misuse of information

and non-transparent processing practices have also intensified [2]. Consequently, the establishment of a robust regulatory framework is essential to ensure secure, transparent, and accountable data management while safeguarding privacy rights, informational autonomy, and broader digital human rights [3]. Indonesia presents distinctive case within global discussions on data governance because, as one of the largest emerging digital economies, it is transitioning from fragmented sectoral regulations toward a comprehensive personal data protection regime through Law No. 27 of 2022 [4]. This development offers an important opportunity to examine how international data protection principles are translated into domestic legal structures within rapidly evolving digital markets [5]. Although previous studies have examined personal data protection from legal and regulatory perspectives, limited attention has been given to the interaction between legal frameworks and the operational realities of Indonesia's digital business ecosystem [6].

Issues related to platform accountability, institutional responsibilities, regulatory harmonization, and practical data governance remain insufficiently explored. Addressing this gap, the present study adopts an integrated legal governance perspective that connects personal data protection with digital platform accountability, public trust, and the sustainability of digital business activities [7]. Accordingly, this research aims to analyze Indonesia's legal framework for personal data protection and identify the major challenges encountered in its implementation across digital business sectors [8]. While the analysis is primarily normative and does not empirically evaluate all digital platforms, the study contributes by proposing a governance-oriented perspective that may enhance regulatory effectiveness, reinforce accountability mechanisms, and inform future policy development concerning personal data protection within Indonesia's digital economy [9].

2. LITERATURE REVIEW

The rapid development of digital technology has transformed various economic sectors, including e-commerce, digital financial services, and other platform-based business models [10]. Within these ecosystems, personal data plays a crucial role in supporting business operations, ranging from user authentication to consumer behavior analysis aimed at improving service quality [11]. The data processed by digital platforms may include user identities, transaction records, geographic information, and consumption preferences [12]. However, the extensive collection and processing of personal data also increase the risks of data breaches, misuse of information, and non-transparent data management practices [13]. Consequently, personal data protection has emerged as a significant issue in digital business law. This literature review explores key concepts and previous studies concerning personal data protection, regulatory frameworks governing digital businesses, data governance, and their implications for the development of the digital economy [14].

2.1. The Concept of Personal Data Protection in the Digital Economy

Personal data protection refers to the legal right of individuals to control how their personal information is collected, used, and disclosed by other parties [15]. In the digital economy, personal data has become a strategic asset that supports service efficiency and data-driven business strategies. Previous studies indicate that the rapid growth of digital activities has significantly increased the volume of personal data collected by technology companies, thereby requiring effective protection mechanisms to prevent privacy violations [16]. Furthermore, personal data protection encompasses not only technical security measures but also legal, ethical, and governance dimensions. Non-transparent data management practices may reduce public trust in digital services and potentially trigger legal disputes between users and service providers [17]. Therefore, effective personal data protection requires the integration of legal regulation, organizational governance, and greater awareness of privacy rights in the digital environment [18].

2.2. Legal Regulations of Personal Data Protection in Indonesia

Indonesia has strengthened its personal data protection framework through the enactment of the Personal Data Protection Law, which regulates the rights of data subjects, the obligations of data controllers, and supervisory mechanisms for data processing [19]. This regulation provides greater legal certainty for digital businesses while enhancing the protection of individual privacy rights [20]. However, its implementation still faces challenges related to organizational readiness, institutional capacity, and coordination among supervisory authorities [21]. Therefore, the effectiveness of the regulation depends largely on robust enforcement mechanisms and effective inter-agency oversight within Indonesia digital business ecosystem [22].

2.3. Data Governance in the Digital Business Ecosystem

Data governance encompasses internal policies that regulate the collection, storage, and use of personal data within digital businesses [23]. Effective data governance enhances information security, reduces the risk of data breaches, and helps maintain public trust and corporate reputation [24]. Conversely, inconsistent implementation of these policies may expose companies to legal risks and diminish user confidence. Therefore, principles such as transparency, accountability, and regulatory compliance are essential components of data governance in the digital business ecosystem [25].

2.4. Personal Data Protection and User Trust

User trust is a crucial factor influencing the success of digital platforms in retaining customers and expanding their market presence [26]. Studies indicate that users are more likely to trust platforms with clear and transparent data protection policies. In this regard, personal data protection serves not only as a legal obligation but also as a strategic asset that enhances corporate reputation [27]. Therefore, strengthening regulations and data governance is essential to maintaining the stability of the digital business ecosystem and fostering public participation in the digital economy [28].

Table 1. Comparison of Previous Studies

References	Year	Research Focus	Key Findings
[2]	2023	Personal data protection law in digital banking governance in Indonesia	Examined the implementation of personal data protection regulations in digital banking and highlighted the importance of legal certainty, customer privacy, and regulatory compliance in financial services.
[5]	2024	Data governance and personal data protection in Indonesia	Proposed strategic data governance practices to strengthen organizational compliance with the Personal Data Protection Law and improve information security management.
[13]	2024	Consumer trust through personal data protection law	Demonstrated that effective implementation of personal data protection regulations enhances consumer trust and provides a competitive advantage for digital businesses.
[19]	2025	Data Protection Impact Assessment (DPIA) framework	Identified critical factors for developing a comprehensive DPIA framework to support privacy risk management and compliance with Indonesia's personal data protection regulations.

Table 1 highlights that personal data protection has become a critical issue in the digital economy. Previous studies emphasize the importance of regulatory frameworks, effective data governance, and transparent data management in enhancing privacy protection, reducing data breach risks, and strengthening user trust [29]. Based on these findings, this study further examines the legal framework of personal data protection within Indonesia digital business ecosystem from a more comprehensive perspective [30].

2.5. Personal Data Protection from the Perspective of the Sustainable Development Goals

The development of the digital economy not only transforms business activities and technological innovation but also intersects with broader sustainable development agendas [31]. The Sustainable Development Goals (SDGs) provide a framework for promoting balanced economic growth, social development, and the protection of community rights [32]. In the context of digital business, personal data protection plays a crucial role in creating a secure, transparent, and accountable digital ecosystem that safeguards individual privacy and supports responsible digital governance [33]. This study is particularly relevant to SDGs 9, which

emphasizes the importance of sustainable infrastructure, innovation, and technological advancement, as well as SDGs 16, which highlights the need for effective institutions, justice, and the protection of individual rights [34]. Therefore, strengthening the legal framework for personal data protection can be viewed as an essential effort to support sustainable digital transformation by fostering trust, enhancing accountability, and ensuring that technological development contributes to a secure, inclusive, and sustainable digital economy [35].

3. RESEARCH METHODS

This study employs a normative legal research approach supported by a regulatory analytical framework to examine Indonesia personal data protection regime within the digital business ecosystem [36]. Primary legal materials consist of statutory regulations related to personal data protection and digital governance in Indonesia, while secondary materials include academic journal articles, legal commentaries, and policy reports published between 2022 and 2025 [37]. Tertiary materials, such as legal dictionaries and institutional publications, are used to support legal interpretation [38]. The analysis was conducted through three stages:

- Identifying relevant legal norms and regulatory instruments governing personal data protection.
- Systematically interpreting these materials to examine their underlying legal principles, regulatory objectives, institutional arrangements, and enforcement mechanisms.
- Synthesizing the findings to assess their alignment with internationally recognized data protection standards and their applicability within Indonesia digital business ecosystem.

Through this analytical process, the study provides a comprehensive legal interpretation of how personal data protection is conceptualized and operationalized in Indonesia, while offering a governance-oriented framework that may guide regulators, courts, and digital platform operators in implementing responsible data governance practices [39].

3.1. Research Approach

This study employs a qualitative approach using a normative juridical method to analyze legal norms governing personal data protection in digital business activities [40]. The analysis focuses on statutory regulations, government policies, and other legal documents related to personal data management, with the Personal Data Protection Law serving as the primary legal basis for examining the rights of data subjects and the obligations of data controllers and processors [41]. Beyond reviewing regulations from a normative perspective, this approach also assesses their relevance and implementation across digital business practices, including e-commerce, digital financial services, and technology-based platforms [42]. Furthermore, it enables the identification of gaps between existing legal provisions and the realities of personal data management within Indonesia evolving digital business ecosystem [43].

3.2. Research Data Sources

In qualitative research, data sources play an important role in supporting a comprehensive analysis process [44]. This study uses two main types of data sources, namely primary data and secondary data. Primary data are obtained from legal documents such as laws, government regulations, and regulatory policies related to personal data protection [45]. Meanwhile, secondary data are obtained from various literature sources such as scientific journals, academic books, research reports, and publications from government institutions and international organizations discussing the development of the digital economy and personal data protection [46].

The data obtained from these various sources are then analyzed systematically to understand how the legal framework for personal data protection is designed and how these regulations interact with digital business practices that are developing in Indonesia [47]. To provide a clearer overview of the types of data sources used in this study, the following table presents the classification of research data sources [48].

Table 2. Classification of Legal Research Data Sources

Data Type	Data source	Information
Primary Data	Regulations and laws and regulations	Used to analyze the legal framework for personal data protection
Secondary Data	The latest scientific journal	Providing an academic perspective on data protection and digital business
Secondary Data	Academic book	Explaining the concept of digital law and data governance
Secondary Data	Institutional Reports	Providing information related to digital economic developments

Table 2 presents the classification of legal research data sources used in this study, including primary legal materials, secondary legal materials, and supporting references relevant to personal data protection governance [49]. Primary data serve as the basis for analyzing the legal framework of personal data protection applicable in Indonesia. Meanwhile, secondary data are used to strengthen the analysis with various academic and empirical perspectives obtained from previous studies. By combining these two types of data, this research is expected to provide a more comprehensive overview of the dynamics of personal data protection within the digital business ecosystem [50].

3.3. Data Collection Techniques

The data collection techniques used in this study were conducted through literature review and document analysis. The literature review was carried out by examining various scientific publications that discuss issues of personal data protection, information technology law, and the development of digital business. Meanwhile, document analysis was conducted by reviewing various laws and regulations, government policies, and official documents related to personal data management.

Through this technique, researchers are able to identify key concepts, relevant theories, and findings from previous studies related to the research topic. In addition, the analysis of legal documents also enables researchers to understand how personal data protection regulations are designed and how these regulations are implemented in digital business activities.



Figure 1. Conceptual research framework illustrating the legal structure and governance dynamics of personal data protection within Indonesia's digital business ecosystem

Figure 1 illustrates the research framework that explains the relationship between legal aspects, personal data protection strategies, and the dynamics of the digital business ecosystem in Indonesia. The framework begins with a qualitative juridical research approach used to analyze various regulations related to personal data protection, such as provisions in laws and regulations as well as policies issued by regulators. Furthermore, the study highlights personal data protection strategies that include privacy policies, data governance, information security, and user access rights as important components in maintaining data security in digital business activities. In the context of the digital business ecosystem, this framework also considers various sectors that utilize user data, such as e-commerce, fintech, social media, and various other digital services that potentially present challenges and risks to personal data security.

This study demonstrates that Indonesia's personal data protection framework plays a crucial role in strengthening digital governance and improving data security within the digital business ecosystem. The findings highlight the importance of regulatory clarity, institutional enforcement, and responsible data management practices to ensure sustainable digital economic growth. Future research should explore empirical evaluations of regulatory implementation and cross-border data governance challenges.

3.4. Data Analysis Techniques

Data analysis in this study was conducted using a descriptive qualitative analysis method. This method aims not only to interpret the collected legal materials but also to systematically evaluate and compare regulatory provisions, including Law No. 27 of 2022, related electronic information regulations, and supporting governance policies. Through this approach, the study analyzes how these regulatory instruments interact in shaping Indonesia's personal data protection framework. The analysis process was carried out through several stages, starting from data reduction, data classification, to drawing conclusions based on the research findings. To provide a more systematic overview of the data analysis process used in this study, the following table presents the stages of data analysis applied in this research.

Table 3. Stages of Data Analysis

Analysis Stages	**Description**
Data Reduction	Selecting and filtering data relevant to the research focus.
Data Categorization	Grouping data by themes such as regulation, data governance, and digital business.
Data Interpretation	Analyzing the relationship between data protection regulations and digital business practices.
Drawing Conclusions	Compiling research findings based on the results of the analysis carried out.

Table 3 presents the stages of data analysis applied in this study, including data reduction, data categorization, and legal interpretation of regulatory provisions related to personal data protection. The first stage is data reduction, which is the process of filtering various pieces of information obtained from data sources so that only data relevant to the research focus are used in the analysis. The second stage is data categorization, which is the process of grouping data based on specific themes or issues such as personal data protection regulations, data governance in digital companies, and challenges in policy implementation. The next stage is data interpretation, which is carried out by analyzing the relationship between the existing legal framework and the practices of personal data management in digital businesses. In the final stage, the researcher formulates conclusions that describe the main findings of the study and provide an understanding of the effectiveness of the personal data protection legal framework in supporting the development of a secure and sustainable digital business ecosystem.

4. RESULTS AND DISCUSSION

The effectiveness of personal data protection regulations in Indonesia is highly dependent on the strength and capacity of institutional enforcement mechanisms. Within the existing regulatory framework, supervisory responsibilities are distributed among several institutions, including the Ministry of Communication and Informatics, sectoral regulatory agencies, and the prospective independent personal data protection authority. While this multi-institutional arrangement is intended to ensure comprehensive oversight, it often creates

coordination challenges, particularly in monitoring compliance across digital platforms and managing cross-border data processing activities. In addition, differences in institutional mandates and operational procedures may lead to inconsistencies in enforcement practices. These challenges become increasingly significant as the volume of personal data processing continues to expand in Indonesia's rapidly growing digital economy. Therefore, establishing clear lines of authority and strengthening inter-agency cooperation are essential steps toward achieving a more effective and coherent personal data protection regime.

4.1. Analysis of the Legal Framework for Personal Data Protection in the Digital Business Ecosystem

The findings show that the growth of Indonesia digital business ecosystem has increased the use of personal data as a strategic asset while also creating challenges related to privacy protection and responsible data management. Existing regulations provide a legal basis for data processing activities and recognize the rights of data subjects, including the rights to information, correction, and data deletion. However, their implementation remains hindered by limited transparency, inadequate security measures, and inconsistent application of data governance principles among digital business actors. Therefore, effective personal data protection requires not only comprehensive regulations but also stronger governance, security mechanisms, consent management, and regulatory supervision to ensure accountability and public trust within the digital ecosystem.

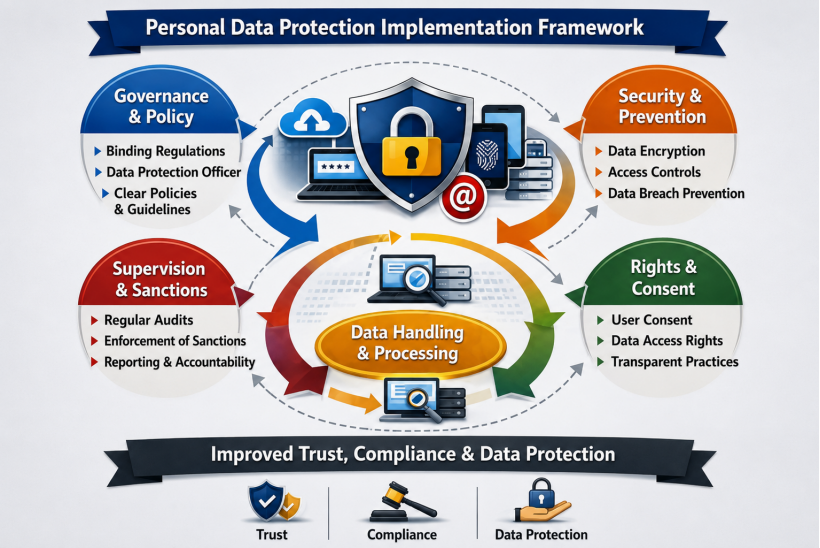


Figure 2. Personal data protection framework integrating governance, security, user rights, and regulatory oversight

Figure 2 High-definition implementation framework illustrating the interaction between governance, security mechanisms, data subject rights, and regulatory supervision in Indonesia's personal data protection regime. The framework highlights how legal obligations translate into operational compliance structures within digital business organizations. The framework places data handling and processing at the center, indicating that all organizational activities involving personal data must follow clear procedures and compliance mechanisms. Surrounding this core are four main pillars: Governance and Policy, which establishes regulations, internal policies, and the role of data protection officers; Security and Prevention, which focuses on technical safeguards such as encryption, access control, and breach prevention; Rights and Consent, which ensures that individuals maintain control over their personal data through consent mechanisms, transparency, and access rights; and Supervision and Sanctions, which includes regulatory monitoring, audits, and enforcement actions to ensure accountability. Together, these interconnected components form a continuous cycle that strengthens trust, legal compliance, and effective personal data protection within the digital ecosystem.

4.2. Implementation of Personal Data Protection on Digital Business Platforms

The research findings further show that the implementation of personal data protection on digital business platforms is strongly influenced by internal company policies as well as the level of organizational awareness regarding the importance of data protection. In practice, digital companies usually adopt various

data protection mechanisms, such as the use of transparent privacy policies, the implementation of encryption technologies, and restrictions on access to user data. These mechanisms aim to prevent the misuse of personal data as well as data breaches that may harm users.

An analysis of data management practices across various digital business sectors shows variations in the level of implementation of personal data protection. Some digital companies have implemented relatively high information security standards, including system security audits and monitoring of data processing activities. However, there are also companies that still face limitations in terms of security infrastructure and data governance policies. This condition indicates that the implementation of personal data protection within the digital business ecosystem remains heterogeneous and requires efforts to harmonize policies at the industry level.

In addition, this study also finds that user trust in digital services is highly influenced by their perception of personal data security. When users feel that their personal data are managed securely and transparently, the level of trust in digital platforms will increase. Conversely, cases of data breaches or misuse of personal information can reduce public trust in digital services.

4.3. Challenges and Risks of Personal Data Protection in the Digital Economy

In the context of the continuously evolving digital economy, personal data protection faces various complex challenges. One of the main challenges is the increasing volume of data generated by society's digital activities. Every user interaction with digital platforms generates various types of data that can be used for consumer behavior analysis as well as the development of digital services. However, the larger the volume of data managed, the higher the risk of data breaches and misuse of personal information.

In addition, the development of digital technologies also introduces new challenges in terms of data security and algorithmic accountability. Technologies such as artificial intelligence, big data analytics, and cloud-based computing systems enable data processing on a very large scale and may affect transparency, fairness, and digital human rights protections. On the one hand, these technologies provide benefits for the efficiency of digital businesses, but on the other hand they also increase the complexity of managing and protecting personal data.

The research findings show that the risks of personal data protection within the digital business ecosystem originate not only from technological factors but also from human and organizational factors. Lack of awareness regarding the importance of data security, weak internal supervision systems, and insufficient understanding of regulations can become factors that increase the risk of violations related to personal data protection.

Table 4. Challenges of Personal Data Protection in the Digital Business Ecosystem

Challenge Aspect	Form of Problem	Impact on the Digital Ecosystem
Regulations	Implementation of regulations is not yet even	Legal uncertainty
Technology	Risk of leaks and cyber attacks	Data security threats
Organization	Data governance is not optimal	Data abuse
User	Lack of digital literacy	Risk of dissemination of personal data

Table 4 shows the various challenges faced in efforts to protect personal data within the digital business ecosystem. These challenges include aspects of regulation, technology, organization, and users. Each aspect has different characteristics of problems and produces specific impacts on the security and sustainability of the digital business ecosystem. Therefore, efforts to protect personal data need to be carried out comprehensively by involving the government, business actors, and the public as users of digital services.

4.4. Implications of Personal Data Protection for Trust and the Sustainability of Digital Business

The research findings show that personal data protection has a strategic role in building public trust in digital business services. User trust is one of the main factors determining the long-term success of digital platforms. When users feel that their personal data are managed securely and responsibly, they tend to be more willing to use digital services and conduct online transactions. In addition, personal data protection also has implications for the sustainability of the digital business ecosystem. Companies that are able to implement effective data governance will have a more positive reputation among users and business partners. This can increase a company's competitiveness in an increasingly competitive digital market. From a sustainable development perspective, personal data protection is also related to efforts to create a digital ecosystem that is secure,

inclusive, and fair. Effective regulations and the proper implementation of data governance can help create a more trustworthy digital environment, thereby supporting the sustainable growth of the digital economy. The proposed conceptual framework is not merely theoretical but can also function as a practical analytical tool for multiple stakeholders within the digital governance ecosystem.

For regulators, the framework can be used to evaluate whether existing data protection regulations effectively balance innovation in digital business with the protection of individual privacy rights. Regulatory bodies may apply the framework to assess compliance mechanisms, identify enforcement gaps, and design adaptive policies that strengthen digital governance. For courts and legal practitioners, the framework offers a structured perspective for interpreting personal data protection disputes by linking legal principles with the broader ecosystem of digital business operations. This perspective helps courts assess liability, accountability, and proportionality when adjudicating cases involving data misuse or digital platform responsibility.

For digital platform operators, the framework can guide the development of internal governance systems such as privacy-by-design policies, transparent data management procedures, and user consent mechanisms. By integrating these governance practices, digital platforms can strengthen user trust while maintaining regulatory compliance and long-term ecosystem sustainability. Through these applications, the framework contributes to bridging the gap between legal doctrine and the operational governance of digital economies.



Figure 3. Conceptual Framework of Personal Data Protection in the Digital Business Ecosystem

Figure 3 The Impact of Personal Data Protection on Trust and Sustainability of the Digital Ecosystem illustrates how effective personal data protection policies contribute to building a secure and sustainable digital environment. Strong data protection practices enhance user confidence, encourage business competitiveness, and ensure regulatory compliance, which collectively strengthen trust between users, companies, and regulators. These protections also support long-term digital development by fostering innovation and growth, reducing risks related to data misuse or cyber threats, and promoting ethical digital practices. As a result, personal data protection not only safeguards individual privacy but also contributes to the resilience, stability, and sustainability of the digital economy and society.

The proposed framework provides practical implications for several institutional actors. For regulators, the framework can serve as a policy reference in designing more coherent personal data protection regulations, supervisory mechanisms, and compliance strategies within digital platform governance. For judicial institutions, the framework offers a structured interpretative approach in assessing legal responsibility related to personal data misuse within digital platforms. Meanwhile, for digital platform operators, the framework highlights the importance of embedding accountability mechanisms, transparency obligations, and compliance strategies aligned with Indonesia's personal data protection law. Through this multidimensional application, the framework bridges normative legal principles with practical governance mechanisms within the digital business ecosystem.

4.5. Normative Legal Framework

From a normative legal perspective, Indonesia's personal data protection regime is primarily grounded in Law No. 27 of 2022 on Personal Data Protection, which establishes fundamental principles governing the collection, processing, storage, and transfer of personal data. These principles include lawfulness, fairness, transparency, purpose limitation, data minimization, accuracy, storage limitation, integrity, and accountability. The law also defines the rights of data subjects and the obligations of data controllers and processors within digital transactions. Normatively, this framework aligns with internationally recognized standards of data governance and reflects Indonesia's commitment to strengthening privacy protection within its digital economy.

4.6. Practical Implementation in Digital Business

In practical terms, however, the implementation of personal data protection within digital business operations remains uneven. Many digital platforms still face challenges in adapting their internal governance systems, including compliance mechanisms, data processing protocols, and risk management procedures. Small and medium-sized digital enterprises often lack adequate legal awareness and technical capacity to fully comply with regulatory requirements. Additionally, the absence of fully operational supervisory institutions during the early implementation phase has created uncertainty regarding enforcement procedures and compliance monitoring. These practical challenges demonstrate the gap between normative legal provisions and operational realities within Indonesia's rapidly growing digital market.

4.7. Implications for Digital Governance

The findings highlight the importance of integrating legal safeguards with technological governance mechanisms. Strong personal data protection frameworks contribute not only to regulatory compliance but also to the long-term stability of digital economies.

5. MANAGERIAL IMPLICATIONS

The findings of this study provide several important managerial implications for organizations and stakeholders involved in the digital business ecosystem. First, digital platform managers need to prioritize strong data governance systems as a strategic component of business operations. Companies should establish clear internal policies related to the collection, storage, processing, and deletion of personal data in accordance with applicable personal data protection regulations. Implementing structured data governance frameworks can help organizations reduce legal risks while ensuring compliance with regulatory requirements.

Second, managers of digital businesses should invest in advanced information security infrastructure to strengthen the protection of user data. The adoption of technologies such as encryption systems, secure authentication mechanisms, access control systems, and continuous security monitoring can significantly reduce the risk of data breaches. In addition, regular security audits and risk assessments are necessary to identify vulnerabilities in digital systems and improve organizational readiness in dealing with potential cyber threats.

Third, companies need to enhance organizational awareness and employee competence regarding personal data protection. Training programs and internal guidelines should be implemented to ensure that employees understand the importance of privacy protection and comply with established data management policies. Strengthening human resource capacity in the area of digital compliance can help organizations minimize operational risks related to personal data misuse.

Fourth, digital businesses should integrate transparency and accountability principles into their data management practices. Clear and easily accessible privacy policies, transparent communication regarding data usage, and effective mechanisms for handling user complaints or data access requests can increase user trust. Organizations that demonstrate responsible data management practices are more likely to build long-term relationships with their users.

In conclusion, the development of Indonesia's personal data protection framework represents an important milestone in strengthening legal governance within the digital business ecosystem. The enactment of Law No. 27 of 2022 provides a formal legal foundation for regulating the collection, processing, and protection of personal data while reinforcing principles of privacy, accountability, and regulatory oversight. However, the effectiveness of this framework depends not only on regulatory design but also on institutional enforcement capacity, organizational compliance readiness, and coordination among supervisory authorities. Strengthening these aspects will be essential to ensure that personal data protection functions effectively as both a legal safeguard for individual rights and a governance mechanism that supports sustainable digital economic growth.

Companies that successfully implement strong data protection systems can strengthen their brand reputation, increase customer loyalty, and enhance their credibility in the digital economy. Therefore, integrating personal data protection into corporate strategy and digital governance frameworks is essential for ensuring the long-term sustainability of digital business operations.

In the broader context of digital governance, personal data protection is increasingly recognized as an essential component of digital human rights. The protection of personal data not only safeguards individual privacy but also reinforces principles of accountability and transparency within digital platforms. As digital transactions frequently transcend national borders, regulatory frameworks must also address issues of cross-border data governance, international legal cooperation, and jurisdictional challenges. Strengthening data protection regimes therefore contributes not only to regulatory compliance but also to the protection of fundamental rights in the digital era, ensuring that technological innovation remains aligned with democratic values and human rights principles.

6. CONCLUSION

In conclusion, the development of personal data protection regulation in Indonesia represents an important legal milestone in the governance of the country's rapidly expanding digital economy. The enactment of Law No. 27 of 2022 has established a comprehensive legal framework that recognizes personal data protection as a fundamental component of digital governance and economic sustainability. The study demonstrates that Indonesia has adopted several internationally recognized principles of data protection, including transparency, accountability, and lawful data processing, which reflect the country's effort to align its regulatory system with global privacy standards.

However, the research also reveals that the effectiveness of this legal framework depends significantly on institutional coordination, enforcement capacity, and the strength of its implementation. Regulatory coordination, supervisory authority, and enforcement capacity remain critical challenges that must be addressed to ensure meaningful protection of personal data within digital business operations. The Indonesian experience illustrates the broader challenge faced by emerging digital economies in translating normative legal commitments into effective governance mechanisms. Future legal research should further examine comparative regulatory models and explore mechanisms for improving enforcement effectiveness within rapidly evolving digital markets. Future legal research should further examine comparative regulatory models and explore mechanisms for improving enforcement effectiveness within rapidly evolving digital markets.

7. DECLARATIONS

7.1. About Authors

Dwi Cahyono (DW) https://orcid.org/0000-0001-9951-560X

Denok Wahyudi Setyo Rahayu (DR) http://orcid.org/0009-0000-6167-6352

Mungkap Mangapul Siahaan (MS) https://orcid.org/0000-0002-8785-1160

John Edwards (JE) https://orcid.org/0009-0004-0067-0490

7.2. Author Contributions

Conceptualization: DW, and JE; Methodology: DR, and MS; Software: MS, and DW; Validation: JE, and DR; Formal Analysis: MS, and DR; Investigation: JE, and DW; Resources: DR; Data Curation: MS, and JE; Writing Original Draft Preparation: DR and JE; Writing Review and Editing: DW, and DR; Visualization: MS; All authors, DW, DR, MS, and JE have read and agreed to the published version of the manuscript.

7.3. Data Availability Statement

The data presented in this study are available on request from the corresponding author.

7.4. Funding

The authors received no financial support for the research, authorship, and/or publication of this article.

7.5. Institutional Review Board Statement

Not applicable.

7.6. Informed Consent Statement

Not applicable.

7.7. Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

REFERENCES

[1] D. D. Wijayanto, K. W. Indrayanti *et al.*, "Personal data protection in digital business based on the law on personal data protection," *International Journal of Research in Social Science and Humanities (IJRSS) ISSN: 2582-6220, DOI: 10.47505/IJRSS*, vol. 6, no. 8, pp. 6–12, 2025.

[2] W. Yuspin, K. Wardiono, A. Nurrahman, and A. Budiono, "Personal data protection law in digital banking governance in indonesia," *Studia Iuridica Lublinensia*, vol. 32, no. 1, pp. 99–130, 2023.

[3] Z. Y. Mubarak and R. N. Triwibowo, "Regulatory transformation of the digital economy and the challenges of personal data protection in indonesia: A literature review," *International Journal of Financial Economics*, vol. 2, no. 1, pp. 187–196, 2025.

[4] B. Prasetyo, I. G. A. K. R. Handayani, and A. Sulistiyono, "Data protection laws in indonesia: Navigating privacy in the digital age," *Side: Scientific Development Journal*, vol. 2, no. 1, pp. 9–16, 2025.

[5] R. Budiarto, I. K. S. Buana, H. Kabetta, H. Setiawan, N. Qomariasih *et al.*, "Enhancing data governance and personal data protection: A strategic review for cases in indonesia," in *2024 International Conference on Informatics, Multimedia, Cyber and Information System (ICIMCIS)*. IEEE, 2024, pp. 625–630.

[6] A. S. Sudarwanto and D. B. B. Kharisma, "Comparative study of personal data protection regulations in indonesia, hong kong and malaysia," *Journal of Financial Crime*, vol. 29, no. 4, pp. 1443–1457, 2022.

[7] I. Lutrianto and R. Riswaldi, "Legal problems of personal data protection in the digital era in personal data protection law in indonesia," *Greenation International Journal of Law and Social Sciences*, vol. 3, no. 2, pp. 345–350, 2025.

[8] I. Hanafi and A. F. Lubis, "Protection of privacy and intellectual property rights in digital data management in indonesia," *The Easta Journal Law and Human Rights*, vol. 2, no. 01, pp. 33–40, 2023.

[9] M. Solikhah, "Personal data protection in the era of digital transformation: Challenges and solutions in the indonesian cyber law framework," *Indonesian Cyber Law Review*, vol. 2, no. 1, pp. 39–50, 2025.

[10] S. Mariyam, A. P. Satria, H. Hariyanto, and A. Masum, "Safeguarding personal data in indonesian e-commerce from a constitutional rights perspective," *Jambe Law Journal*, vol. 8, no. 2, pp. 683–711, 2025.

[11] U. Rahardja, M. T. D. S. Putri, N. Septiani, F. Amelia, A. Avandi, and R. Evans, "Human centered legal governance for autonomous ai in digital societies," *Legal Autonomous Web-based Governance (LAW)*, vol. 1, no. 1, pp. 29–41, 2026.

[12] I. Rahman, M. H. Muhtar, N. M. Mongdong, R. Setiawan, B. Setiawan, and H. K. Siburian, "Harmonization of digital laws and adaptation strategies in indonesia focusing on e-commerce and digital transactions," *Innovative: Journal Of Social Science Research*, vol. 4, no. 1, pp. 4314–4327, 2024.

[13] R. A. Prastyanti and R. Sharma, "Establishing consumer trust through data protection law as a competitive advantage in indonesia and india," *Journal of Human Rights, Culture and Legal System*, vol. 4, no. 2, pp. 354–390, 2024.

[14] A. A. Nugraha and A. H. Nasyuha, "Integrating iso 27001 and indonesia's personal data protection law for data protection requirement model," *Journal of Information Systems and Informatics*, vol. 6, no. 2, pp. 1052–1069, 2024.

[15] L. Meria, M. S. Gunawan, S. Solahudin, U. Rahardja, and A. Patel, "Enhancing digital business students competence through ui/ux design training for digital product development," *ADI Pengabdian Kepada Masyarakat*, vol. 6, no. 2, pp. 133–144, 2026.

[16] F. Rahman, "Safeguarding personal data in the public sector: Unveiling the impact of the new personal data protection act in indonesia," *UUM Journal of Legal Studies*, vol. 16, no. 1, pp. 1–18, 2025.

[17] A. Marwan and F. Bonfigli, "Detection of digital law issues and implication for good governance policy in indonesia," *Bestuur*, vol. 10, no. 1, pp. 22–32, 2022.

[18] E. Santoso *et al.*, "Opportunities and challenges: e-commerce in indonesia from a legal perspective," *Jurnal Penelitian Hukum De Jure*, vol. 22, no. 3, pp. 395–410, 2022.

[19] S. Prabowo, M. Abdurohman, H. H. Nuha, and S. Sutikno, "Identifying and validating critical factors in designing a comprehensive data protection impact assessment (dpia) framework for indonesia." *International Journal of Safety & Security Engineering*, vol. 15, no. 1, 2025.

[20] Indonesian National Police. (2025, Jan.) Govt. to harmonize presidential decree in strengthening personal data protection. Indonesian National Police (INP). Accessed: 15 June 2026. [Online]. Available: https://inp.polri.go.id/artikel/govt-to-harmonize-presidential-decree-in-strengthening-personal-data-protection

[21] U. Rahardja, M. A. Ngad, S. Millah, E. P. Harahap, and Q. Aini, "Blockchain application in educational certificates and verification compliant with general data protection regulations," in *2022 10th International Conference on Cyber and IT Service Management (CITSM)*. IEEE, 2022, pp. 1–7.

[22] F. Sugianto, E. Sukardi, and T. Michael, "Comparison of legal consumer protection systems in e-commerce transactions to support digital economic growth in indonesia," *Dalat University Journal of Science*, pp. 39–51, 2022.

[23] M. Hafel *et al.*, "Digital transformation in politics and governance in indonesia: Opportunities and challenges in the era of technological disruption," *Society*, vol. 11, no. 2, pp. 742–757, 2023.

[24] D. S. Gojali, "Identifying the prevalence of cybercrime in indonesian corporations: A corporate legislation perspective," *International Journal of Cyber Criminology*, vol. 17, no. 1, pp. 1–11, 2023.

[25] S. W. Dyatmika, B. Suyanto, E. Setijaningrum, A. Rizky, and T. Mkhize, "Enhancing brand loyalty through customer satisfaction strategies in digital business," *Aptisi Transactions on Technopreneurship (ATT)*, vol. 7, no. 2, pp. 556–566, 2025.

[26] M. K. Hamsin, A. Halim, R. Anggriawan, and H. Lutfiani, "Sharia e-wallet: The issue of sharia compliance and data protection." *Al-Manahij: Jurnal Kajian Hukum Islam*, vol. 17, no. 1, p. 53, 2023.

[27] Z. Morić, V. Dakic, D. Djekic, and D. Regvart, "Protection of personal data in the context of e-commerce," *Journal of cybersecurity and privacy*, vol. 4, no. 3, pp. 731–761, 2024.

[28] A. Kristian, A. Supriyadi, R. Sean, A. Husain *et al.*, "Exploring the relationship between financial competence and entrepreneurial ambitions in digital business education," *APTISI Transactions on Management*, vol. 8, no. 2, pp. 139–145, 2024.

[29] M. Lubis and D. O. D. Handayani, "The relationship of personal data protection towards internet addiction: Cyber crimes, pornography and reduced physical activity," *Procedia Computer Science*, vol. 197, pp. 151–161, 2022.

[30] I. Amarini, Y. Saefudin, I. A. Kartini, M. Marsitiningsih, and N. Ismail, "Digital transformation: creating an effective and efficient court in indonesia," *Legality: Jurnal Ilmiah Hukum*, vol. 31, no. 2, pp. 266–284, 2023.

[31] I. Anwary, "The role of public administration in combating cybercrime: An analysis of the legal framework in indonesia," *International Journal of Cyber Criminology*, vol. 16, no. 2, pp. 216–227, 2022.

[32] D. Cahyono, A. Susbiyani, E. Lestari, F. Fauziyah, N. Qomariah, and Y. S. Guntur, "Role of personal savings in financial tech impact on family planning in indonesia," *Aptisi Transactions on Technopreneurship (ATT)*, vol. 7, no. 1, pp. 120–131, 2025.

[33] D. S. Negara and D. Darmawan, "Digital empowerment: Ensuring legal protections for online arisan engagements," *Bulletin of Science, Technology and Society*, vol. 2, no. 2, pp. 13–19, 2023.

[34] R. Wagola, A. Nurmandi, Misran, and D. Subekti, "Government digital transformation in indonesia," in *International Conference on Human-Computer Interaction*. Springer, 2023, pp. 286–296.

[35] R. Widayanti, A. B. Mutiara, and A. Tarigan, "Data governance in blockchain-based systems for internship grade conversion," *Aptisi Transactions on Technopreneurship (ATT)*, vol. 6, no. 3, pp. 509–521, 2024.

[36] A. T. Oyewole, B. B. Oguejiofor, N. E. Eneh, C. U. Akpuokwe, and S. S. Bakare, "Data privacy laws and their impact on financial technology companies: a review," *Computer science & IT research journal*, vol. 5, no. 3, pp. 628–650, 2024.

[37] T. Anas and E. Cahyawati, "Strategic investment policies for digital transformation," *Journal of Southeast Asian Economies*, vol. 40, no. 1, pp. 96–126, 2023.

[38] A. Bist, N. Zakaria, N. Anwar, G. Jacqueline, and L. MING, "Future of work: How digital tools are transforming human resource management," *APTISI TRANSACTIONS ON MANAGEMENT: iLearning Journal Center*, vol. 8, no. 3, pp. 213–220, 2024.

[39] E. Coche, A. Kolk, and V. Ocelík, "Unravelling cross-country regulatory intricacies of data governance: the relevance of legal insights for digitalization and international business," *Journal of International Business Policy*, vol. 7, no. 1, pp. 112–127, 2024.

[40] N. Siagian, "Leveraging digital business communication for enhanced profitability in global markets," in *Proceedings of International Conference on Social, Politics, Administration, and Communication Sciences*, vol. 1, no. 2, 2024, pp. 94–110.

[41] S. W. Gusman, "Development of the indonesian government's digital transformation," *Dinasti International Journal of Education Management And Social Science*, vol. 5, no. 5, pp. 1128–1141, 2024.

[42] T. Sendjaja, D. J. Rachbini, R. Astini, and D. Asih, "Driving socialpreneurship and diving into digital transformation to enhance donation intentions in indonesia," *Aptisi Transactions on Technopreneurship (ATT)*, vol. 7, no. 3, pp. 687–700, 2025.

[43] A. Noor, H. Ahamat, I. Marzuki, D. Wulandari, A. A. Junaidi, E. Lisdiyono, and B. Trisnawati, "Regulation and consumer protection of fintech in indonesia: The case of islamic fintech lending," *Linguistics and Culture Review*, vol. 6, no. on, pp. 49–63, 2022.

[44] A. Prayitno, "Technological innovation in public administration transformation: Case study of e-government implementation in indonesia," *Journal of Governance*, vol. 8, no. 4, pp. 628–642, 2023.

[45] A. Rizky, R. W. Nugroho, W. Sejati, O. Sy *et al.*, "Optimizing blockchain digital signature security in driving innovation and sustainable infrastructure," *Blockchain Frontier Technology*, vol. 4, no. 2, pp. 183–192, 2025.

[46] B.-K. Cheryl and B.-K. Ng, "Protecting the unprotected consumer data in internet of things: Current scenario of data governance in malaysia," *Sustainability*, vol. 14, no. 16, p. 9893, 2022.

[47] A. Amruddin, A. Safari, E. Masita, R. Indrawati, and E. Y. Utami, "The urgency of digital business in improving the rural community youth organization's business," *Journal Of Human And Education (JAHE)*, vol. 4, no. 1, pp. 70–75, 2024.

[48] G. Simuni and A. Atla, "Hadoop in enterprise data governance: Ensuring compliance and data integrity," *Available at SSRN 4982500*, 2024.

[49] M. A. W. Saputra, D. Ochtaffia, D. Apriani, S. C. Yusfi, and M. Gori, "Blockchain applications in education affecting challenges and problems in digital," *Blockchain Frontier Technology*, vol. 2, no. 2, pp. 15–23, 2023.

[50] I. Anwary, "Evaluating legal frameworks for cybercrime in indonesian public administration: An interdisciplinary approach," *International Journal of Cyber Criminology*, vol. 17, no. 1, pp. 12–22, 2023.