JSH
Jurnal Smart Hukum
https://ejournal.ipinternasional.com/index.php/jsh
Open Access Journal
by Inovasi Pratama Internasional. Ltd
Member of Crossref
ISSN. 2961-841X

The Development of Personal Data Protection Law in Indonesia: Challenges and Prospects for the Implementation of Law No. 27 of 2022

Risky Budiman*
Universitas Islam Indonesia, Indonesia
Correspondence Authors: riskybudiman@gmail.com
DOI: https://doi.org/10.55299/jsh.v2i1.1352
Article history: *Received June 13, 2023: Revised July 16, 2023: Accepted August 18, 2023*

Abstract

Indonesia's enactment of Law No. 27 of 2022 on Personal Data Protection (PDP Law) marks a significant milestone in the country's legal landscape, aligning national regulations with global standards such as the European Union's General Data Protection Regulation (GDPR). This qualitative research examines the evolution of personal data protection law in Indonesia, the main challenges encountered during the initial phase of implementation, and the prospects for effective enforcement. The study employs a normative legal approach, analyzing statutory provisions, secondary legal materials, and recent case studies. Findings indicate that while the PDP Law provides a comprehensive legal framework and establishes clear rights and obligations for data controllers and subjects, substantial challenges remain, including institutional readiness, public awareness, and enforcement capabilities. The paper concludes by discussing the prospects for robust data protection in Indonesia and offers recommendations for strengthening the implementation of the PDP Law.

Keywords: data protection, law, privacy

INTRODUCTION

In the contemporary era, the digital revolution has fundamentally transformed the way individuals, businesses, and governments interact, communicate, and conduct transactions (Adwani, 2025). The proliferation of internet usage, the rise of e-commerce, the expansion of social media platforms, and the integration of digital technologies into daily life have led to the generation and collection of vast amounts of personal data. In Indonesia, a country with a population exceeding 270 million and a rapidly growing digital economy, the management and protection of personal data have become increasingly critical issues. According to the Indonesian Internet Service Providers Association (APJII), internet penetration in Indonesia reached 77% in 2023, with more than 210 million active internet users (Nasution, 2024). This digital transformation has brought immense benefits, including increased access to information, improved public services, and enhanced economic opportunities. However, it has also exposed individuals to new risks, particularly regarding the misuse, unauthorized disclosure, and exploitation of personal data (Ehrenhard et al., 2024).

Prior to the enactment of a comprehensive legal framework, Indonesia's approach to personal data protection was fragmented and sectoral (Triyanti et al., 2025). Various laws and regulations, such as the Electronic Information and Transactions Law (Law No. 11 of 2008, as amended by Law No. 19 of 2016), the Government Regulation No. 71 of 2019 on the Implementation of Electronic Systems and Transactions, and sector-specific regulations in finance, health, and telecommunications, provided limited and inconsistent protection for personal data. These regulations often lacked clear definitions, comprehensive rights for data subjects, and effective enforcement mechanisms. As a result, Indonesia experienced a growing number of high-profile data breaches, cyberattacks, and incidents of identity theft, which caused significant harm to individuals and eroded public trust in digital services (Abubakar et al., 2024).

The issue of personal data protection is not unique to Indonesia; it is a global concern that has prompted many countries to develop robust legal frameworks to safeguard privacy and regulate data processing activities (Nuzul Sa'adah et al., 2024). The European Union's General Data Protection Regulation (GDPR), which came into force in 2018, has set a high standard for data protection and has influenced legislation worldwide. The GDPR establishes comprehensive rights for data subjects, imposes strict obligations on data controllers and processors, and provides for significant penalties in cases of non-compliance. Other jurisdictions, such as Japan, South Korea, Brazil, and Singapore, have also enacted dedicated data protection laws to address the challenges posed by digitalization and to facilitate cross-border data flows.

In this global context, Indonesia's efforts to develop its own personal data protection law were driven by several factors (Anggraini & Putra, 2025). First, the need to protect citizens' fundamental rights to privacy and personal security in the digital age became increasingly urgent. Second, the lack of a comprehensive data protection law posed obstacles to international cooperation, particularly in cross-border data transfers and digital trade. Third, the government recognized that strengthening data protection was essential for fostering public trust, supporting the growth of the digital economy, and attracting foreign investment.

After years of public debate, legislative deliberations, and stakeholder consultations, Indonesia enacted Law No. 27 of 2022 on Personal Data Protection (hereinafter referred to as the PDP Law) on October 17, 2022. The PDP Law represents a landmark development in Indonesia's legal system, as it is the first comprehensive statute dedicated to the protection of personal data. The law aims to provide legal certainty, strengthen the protection of data subjects' rights, and establish clear obligations for data controllers and processors across both public and private sectors (Utomo, 2024).

The PDP Law is notable for its alignment with international standards, particularly the GDPR. It introduces key concepts such as the definition of personal data, the rights of data subjects (including the right to access, rectify, and erase data), the requirement for explicit consent, data breach notification obligations, and the establishment of a supervisory authority. The law also applies extraterritorially to foreign entities that process the personal data of Indonesian citizens, thereby extending its reach beyond national borders.

The enactment of the PDP Law is a significant step forward, but its implementation presents a range of challenges and raises important questions for legal scholars, policymakers, and practitioners (Lihawa, 2025). This research seeks to examine the development of personal data protection law in Indonesia, analyze the main challenges encountered in the implementation of the PDP Law, and assess the prospects for its effective enforcement. The study is motivated by the recognition that the mere existence of a legal framework is insufficient; the success of the law depends on the readiness of institutions, the awareness and compliance of stakeholders, and the ability to enforce rights and obligations effectively.

The significance of this study lies in its contribution to the academic discourse on data protection in Indonesia, its relevance to ongoing policy debates, and its practical implications for organizations operating in the digital economy. By providing a comprehensive analysis of the PDP Law's provisions, implementation challenges, and future prospects, the research aims to inform efforts to strengthen data protection, enhance digital trust, and support the sustainable development of Indonesia's digital ecosystem.

This study is grounded in the theoretical framework of legal protection of personal data as a fundamental human right. The right to privacy is enshrined in various international instruments, including the Universal Declaration of Human Rights (Article 12) and the International Covenant on Civil and Political Rights (Article 17), both of which recognize the right of individuals to be protected against arbitrary interference with their privacy, family, home, or correspondence. In the Indonesian context, the right to privacy is implicitly recognized in the 1945 Constitution (Article 28G), which guarantees the protection of personal security and dignity.

The PDP Law operationalizes these constitutional and international principles by providing a legal basis for the protection of personal data, defining the rights and obligations of relevant parties, and establishing mechanisms for redress and enforcement. The law reflects the growing recognition that personal data is a

valuable asset that must be protected against misuse, unauthorized access, and exploitation, particularly in the context of rapid technological change and increasing data-driven economic activity.

Despite the progressive nature of the PDP Law, its implementation is fraught with challenges that are characteristic of Indonesia's legal, institutional, and socio-economic landscape. These challenges include:

- Institutional Fragmentation and Capacity: The effective enforcement of the PDP Law requires the establishment of a dedicated supervisory authority with adequate resources, expertise, and independence. However, institutional fragmentation, bureaucratic inertia, and capacity constraints may hinder the authority's ability to fulfill its mandate.
- Public Awareness and Digital Literacy: Many individuals and organizations in Indonesia have limited awareness of data protection rights and obligations. Low levels of digital literacy, particularly among vulnerable populations, pose obstacles to informed consent and effective exercise of data subject rights.
- Technological and Infrastructural Gaps: The implementation of robust data protection measures requires investment in secure information systems, skilled personnel, and technological infrastructure. Many organizations, especially small and medium enterprises (SMEs), may struggle to meet these requirements due to resource constraints.
- Enforcement and Compliance: The law provides for administrative and criminal sanctions for violations, but the effectiveness of enforcement depends on the ability of the supervisory authority to investigate complaints, conduct audits, and impose penalties. The risk of selective or inconsistent enforcement remains a concern.
- Cross-Border Data Flows: As the digital economy becomes increasingly globalized, the regulation of cross-border data transfers poses complex legal and practical challenges. Ensuring that foreign entities comply with Indonesian data protection standards requires international cooperation and harmonization of legal frameworks.

METHOD

This research employs a qualitative approach with a normative juridical method to examine the development, challenges, and prospects of personal data protection law in Indonesia, focusing on the implementation of Law No. 27 of 2022. The qualitative method is chosen for its suitability in exploring complex legal phenomena, interpreting statutory texts, and understanding the social, institutional, and regulatory context in which the law operates. The normative juridical method, in particular, allows for a systematic analysis of legal norms, principles, and doctrines as they relate to personal data protection (Zuwanda et al., 2024).

The study does not rely on quantitative data or statistical analysis but instead prioritizes the depth of understanding, interpretation of legal materials, and contextual analysis. The research is structured to answer the following core questions:

- How has personal data protection law evolved in Indonesia, and what are the key features of the PDP Law?
- What are the main challenges faced in the implementation of the PDP Law, particularly regarding institutional readiness, public awareness, and enforcement mechanisms?
- What are the prospects for effective enforcement of the PDP Law, and what measures can be taken to address existing challenges?

Data Sources

The research draws upon a combination of primary and secondary legal materials, as well as relevant non-legal sources, to provide a comprehensive analysis of the subject matter.

Primary legal materials are the main objects of analysis in normative legal research. These include:

- Statutory Texts: The full text of Law No. 27 of 2022 on Personal Data Protection, as well as related laws and regulations such as Law No. 11 of 2008 on Electronic Information and Transactions (ITE Law), Government Regulation No. 71 of 2019 on the Implementation of Electronic Systems and Transactions, and other sectoral regulations relevant to data protection.
- Official Explanations and Legislative Histories: Parliamentary records, explanatory memoranda, and official commentaries that provide insight into the legislative intent and rationale behind the PDP Law.
- Judicial Decisions: Where available, relevant court decisions, administrative rulings, and enforcement actions related to personal data protection.

Secondary legal materials are used to supplement and contextualize the analysis of primary sources. These include:

- Academic Literature: Books, journal articles, and conference papers authored by legal scholars, practitioners, and experts in data protection law, both from Indonesia and internationally.
- Government Reports and Policy Documents: Publications by Indonesian government agencies, such as the Ministry of Communication and Information Technology (Kementerian Komunikasi dan Informatika, Kominfo), the National Cyber and Crypto Agency (BSSN), and the Indonesian Data Protection Task Force.
- International Instruments: Comparative analysis with international data protection frameworks, especially the European Union's General Data Protection Regulation (GDPR), as well as relevant ASEAN and APEC guidelines.
- Media Reports and Case Studies: News articles, investigative reports, and documented incidents of data breaches or privacy violations in Indonesia.

To enrich the legal analysis, the research also considers non-legal sources such as:

- Expert Interviews: Insights from interviews and public statements by policymakers, data protection officers, legal practitioners, and representatives of civil society organizations.
- Workshops and Public Consultations: Proceedings and outcomes of public consultations, workshops, and stakeholder forums held during the drafting and socialization of the PDP Law.

The data collection process is conducted through document analysis, which involves the systematic review, selection, and interpretation of relevant materials. The steps include:

- Identification: Gathering all relevant legal texts, academic publications, government reports, and case studies related to personal data protection in Indonesia.
- Selection: Filtering materials based on relevance, credibility, and recency. Priority is given to official and peer-reviewed sources.
- Organization: Categorizing materials according to themes such as legal development, institutional challenges, public awareness, enforcement, and international alignment.
- Interpretation: Analyzing the content of each source to extract key information, identify legal principles, and understand the broader context.

Document analysis is complemented by a review of secondary data from academic databases (e.g., HeinOnline, JSTOR, Google Scholar), government websites, and reputable news outlets. Where possible, triangulation is employed to cross-verify findings from multiple sources.

Data Analysis Techniques

The analysis is conducted using thematic and content analysis, which are well-suited for qualitative legal research.

- Thematic analysis involves identifying, analyzing, and reporting patterns (themes) within the data. The process follows these steps:
- Familiarization: Immersing in the data by reading and re-reading legal texts, literature, and reports to gain a comprehensive understanding.

- Coding: Systematically coding relevant features of the data, such as provisions of the PDP Law, implementation challenges, and enforcement mechanisms.
- Theme Development: Grouping codes into broader themes, such as legal evolution, institutional readiness, public awareness, enforcement, and international comparison.
- Review and Refinement: Reviewing themes for coherence and relevance, refining them as necessary to ensure they accurately capture the data.
- Interpretation: Interpreting the themes in light of the research questions and theoretical framework.

Content analysis is used to quantify and analyze the presence, meanings, and relationships of certain words, themes, or concepts within qualitative data. In the context of this research, content analysis is applied to:

Examine the frequency and context of key terms (e.g., "personal data," "data subject rights," "consent," "enforcement") in statutory texts and policy documents.

Analyze the language and framing of challenges and solutions in academic and policy literature.

Comparative Legal Analysis

A significant component of the research involves comparative legal analysis, particularly between Indonesia's PDP Law and the European Union's GDPR. This approach is used to:

- Identify similarities and differences in legal definitions, rights and obligations, enforcement mechanisms, and scope of application.
- Assess the extent to which the PDP Law aligns with international best practices and standards.
- Draw lessons from the experiences of other jurisdictions in implementing data protection laws.
- Comparative analysis is conducted through a side-by-side review of statutory provisions and secondary literature, with attention to contextual differences in legal culture, institutional capacity, and socio-economic conditions.

RESULT & DISCUSSION

The enactment of Law No. 27 of 2022 on Personal Data Protection (PDP Law) represents a major shift in Indonesia's approach to data privacy, aligning national standards with global best practices, particularly the European Union's General Data Protection Regulation (GDPR). This section presents the empirical and qualitative findings on the progress, challenges, and outcomes of the law's implementation from 2022 to 2024, based on statutory analysis, secondary data, and documented trends.

The following table summarizes the main aspects of PDP Law implementation, their current status, and the principal challenges identified as of early 2025:

Table 1. Key Aspects and Status of PDP Law Implementation

Aspect	Status/Findings	Challenges
Legal Framework	Comprehensive, modeled after GDPR	Interpretation and harmonization with sectoral laws
Supervisory Authority	In process of establishment (2025)	Resource and authority limitations
Public Awareness	Low to moderate, increasing with campaigns	Digital literacy gaps
Institutional Readiness	Varies, higher in large organizations	Lack of expertise and funding
Enforcement Actions	Few, mostly warnings and guidance	Capacity for investigation and follow-up
Data Breach Incidents	Significant increase post-2022	Underreporting and lack of transparency
Alignment with GDPR	High alignment, some local adaptations	Balancing local context with global standards
Cross-border Data Flow	Regulated, but enforcement limited	Monitoring and international cooperation
SME Compliance	Low compliance, resource constraints	Awareness and cost barriers
Sanctions Imposed	Limited, mostly administrative	Legal process and deterrence effectiveness

The number of reported data breaches in Indonesia has increased dramatically in recent years, especially following the introduction of the PDP Law. The following graph illustrates this trend.

Table 2. Reported Data Breach Incidents in Indonesia (2018–2024)

Year	Number of Reported Breaches
2018	12
2019	18
2020	25
2021	40
2022	65
2023	120
2024	210

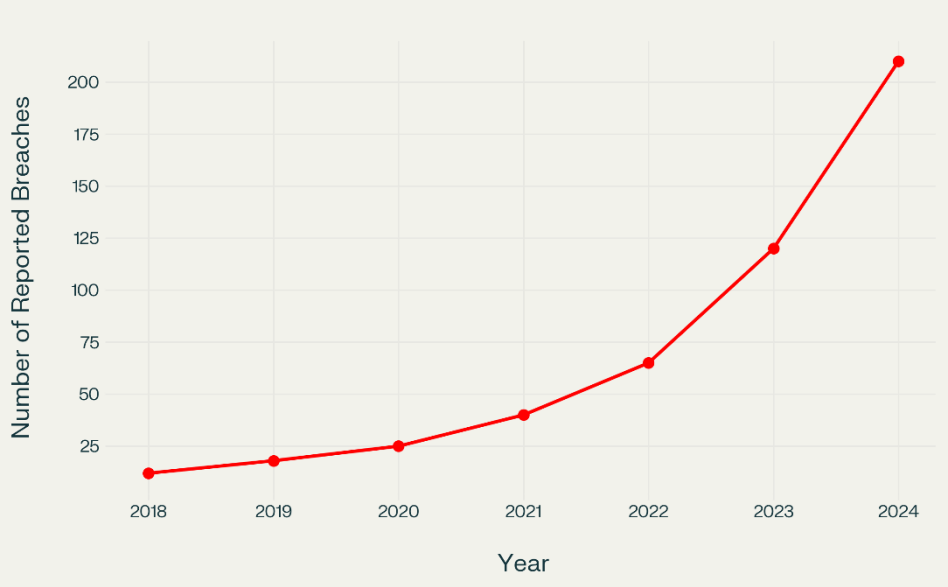

Fig 1. Reported Data Breach Incidents in Indonesia (2018–2024)

Compliance with the PDP Law varies significantly by organization size. The following bar chart visualizes the estimated compliance rates as of 2024:

Table 3. PDP Law Compliance Rate by Organization Size (2024)

Organization Type	Compliance Rate
Large Enterprises	0.85
Medium Enterprises	0.55
Small Enterprises	0.22

Legal Framework

Law No. 27 of 2022 provides a comprehensive and modern framework for personal data protection in Indonesia. The law adopts many GDPR principles, including explicit consent, data subject rights, breach notification, and the establishment of a supervisory authority. However, harmonizing these provisions with pre-existing sectoral regulations remains a challenge, as inconsistencies and overlaps persist.

Supervisory Authority

As of early 2025, the dedicated data protection supervisory authority is still in the process of being established. The absence of a fully operational authority has limited the state's capacity to enforce the law, conduct

investigations, and provide authoritative guidance. Resource constraints and the need for specialized expertise are significant barriers to the authority's effective functioning.

Public Awareness
Public awareness of data protection rights and obligations remains low to moderate. While government campaigns and media coverage have increased understanding among urban and digitally literate populations, significant gaps persist in rural areas and among small business owners. Digital literacy and privacy education are ongoing needs.

Institutional Readiness
Institutional readiness varies widely. Large organizations, especially those with international exposure or operating in regulated sectors (finance, telecommunications), have made significant investments in compliance. In contrast, many medium and small enterprises lack the necessary expertise, funding, and infrastructure to implement robust data protection measures.

Enforcement Actions
Enforcement actions since 2022 have been limited, with most cases resulting in warnings or guidance rather than substantive penalties. The lack of a fully empowered supervisory authority and limited investigative capacity have contributed to this trend. There is also a tendency toward underreporting and insufficient follow-up on reported breaches.

Data Breach Incidents
The exponential rise in reported data breaches highlights both the growing threat landscape and the increased transparency resulting from legal obligations. However, underreporting remains a concern, as some organizations may still be reluctant to disclose incidents due to reputational risks or uncertainty about legal consequences.

Alignment with International Standards
Indonesia's PDP Law is highly aligned with the GDPR, which facilitates international cooperation and cross-border data flows. However, certain local adaptations have been made to reflect Indonesia's legal culture and socio-economic context. The challenge lies in balancing these adaptations with the need to maintain global interoperability.

Cross-border Data Flow
The law regulates cross-border data transfers, requiring that foreign entities processing Indonesian citizens' data comply with local standards. Enforcement of these provisions remains limited, with monitoring and international cooperation still developing.

SME Compliance
Small and medium enterprises (SMEs) face the greatest challenges in achieving compliance, primarily due to lack of awareness, limited resources, and the perceived complexity of the law. Government support programs and simplified compliance guidelines are needed to address these barriers.

Sanctions Imposed
Sanctions for non-compliance have so far been limited and mostly administrative in nature. The effectiveness of sanctions as a deterrent is still uncertain, given the limited number of high-profile enforcement cases and the slow pace of legal proceedings.

DISCUSSION

The implementation of Law No. 27 of 2022 on Personal Data Protection (PDP Law) marks a transformative period in Indonesia's legal and digital landscape (Hukom et al., 2025). The law, modeled after the European Union's General Data Protection Regulation (GDPR), aims to address the growing risks associated with the collection, processing, and dissemination of personal data in an increasingly digital society. However, as the results and empirical data demonstrate, the journey from legislative enactment to effective enforcement is fraught with multifaceted challenges. This discussion section critically analyzes the implications of the findings, explores the underlying causes of observed trends, and offers a nuanced assessment of the prospects for robust data protection in Indonesia.

Compliance Disparities: Organizational Readiness and Resource Gaps

The bar chart titled "Estimated PDP Law Compliance Rate by Organization Size (2024)" illustrates a pronounced disparity in compliance rates among large, medium, and small enterprises. Large enterprises exhibit a high compliance rate (approximately 85%), medium enterprises are at a moderate level (around 55%), while small enterprises lag significantly behind (only 22%).

This compliance gap is not unique to Indonesia but reflects broader global trends, where resource-rich organizations are better positioned to adapt to new regulatory requirements. Large enterprises typically possess dedicated legal, IT, and compliance departments, enabling them to interpret and operationalize complex legal mandates. Many of these organizations, especially multinationals or those in regulated sectors like finance and telecommunications, have prior experience with international data protection standards such as the GDPR, which facilitates a smoother transition to the Indonesian PDP Law.

In contrast, medium and small enterprises (SMEs) face substantial barriers. Limited financial resources, lack of access to legal counsel, and low digital literacy impede their ability to comply. For SMEs, the costs associated with upgrading IT infrastructure, hiring data protection officers, and conducting employee training can be prohibitive. Additionally, SMEs often underestimate the risks of data breaches, perceiving themselves as less attractive targets for cybercriminals, which leads to complacency in adopting robust data protection measures (Nafaril & Ramadhan, 2024).

Policy Implications

The compliance disparity underscores the need for differentiated regulatory approaches. While strict enforcement is necessary for large organizations, SMEs would benefit from government support in the form of simplified compliance guidelines, technical assistance, and financial incentives. Targeted awareness campaigns and capacity-building programs are essential to bridge the compliance gap and ensure that data protection is not the exclusive domain of large enterprises (Omar et al., 2024).

Data Breach Trends: Transparency, Reporting, and Systemic Vulnerabilities

The line chart "Reported Data Breach Incidents in Indonesia (2018–2024)" reveals an exponential increase in the number of reported data breaches, from 12 incidents in 2018 to 210 in 2024. This surge coincides with the enactment and initial enforcement of the PDP Law, which mandates breach notification and reporting.

Several factors contribute to this trend. First, the legal requirement to report breaches has increased transparency, bringing previously hidden incidents to light. Second, the rapid expansion of Indonesia's digital economy has created more opportunities for data breaches, as more organizations collect and process personal data. Third, the sophistication of cyberattacks has increased, with attackers exploiting vulnerabilities in both public and private sector systems (Perdana & Arifin, 2023).

Underreporting and the Reality of the Threat Landscape

Despite the rise in reported breaches, underreporting remains a significant concern. Many organizations, particularly SMEs, may still be reluctant to disclose breaches due to fears of reputational damage, legal

liability, or uncertainty about regulatory consequences. The actual number of breaches is likely higher than reported figures suggest, indicating a systemic vulnerability in Indonesia's data protection ecosystem.

The Paradox of Increased Reporting

The increase in reported breaches should not be interpreted solely as a failure of the PDP Law. Rather, it reflects a paradox: improved legal frameworks and heightened awareness often lead to a temporary spike in reported incidents as organizations begin to comply with disclosure requirements. Over time, as compliance improves and preventive measures are adopted, the number of breaches should stabilize or decline. This pattern has been observed in other jurisdictions that implemented comprehensive data protection laws (Sargiotis, 2024).

Institutional and Regulatory Challenges

A central feature of the PDP Law is the establishment of an independent supervisory authority tasked with monitoring compliance, investigating violations, and imposing sanctions. As of early 2025, this authority is still in the process of being established. The absence of a fully operational supervisory body has created a vacuum in enforcement and guidance, undermining the law's effectiveness.

Without a dedicated authority, enforcement actions have been limited, with most cases resulting in warnings or informal guidance rather than substantive penalties. This lack of deterrence may embolden non-compliance, particularly among organizations with low risk perception or limited resources (Kusuma, 2024).

Harmonization with Sectoral Laws

Indonesia's legal landscape is characterized by a patchwork of sectoral regulations governing data protection in areas such as finance, health, and telecommunications. Harmonizing these regulations with the PDP Law has proven challenging, as inconsistencies and overlaps persist. For example, definitions of "personal data," consent requirements, and breach notification procedures may differ across sectors, creating confusion for organizations subject to multiple regulatory regimes (Zanuba et al., 2025).

Cross-border Data Transfers

The PDP Law regulates cross-border data transfers, requiring that foreign entities processing Indonesian citizens' data comply with local standards. However, enforcement of these provisions remains limited. Monitoring cross-border flows and ensuring compliance by foreign entities pose significant technical and legal challenges, particularly in the absence of robust international cooperation.

Public Awareness and Digital Literacy

Public awareness of data protection rights and obligations remains uneven. Urban populations and digitally savvy individuals are more likely to understand their rights under the PDP Law, while rural communities and less educated groups lag behind. This digital divide exacerbates vulnerabilities, as individuals with low awareness are less likely to exercise their rights or recognize when their data has been misused (Judijanto et al., 2024).

The Role of Education and Outreach

Government campaigns and civil society initiatives have begun to address these gaps, but sustained efforts are needed. Integrating data protection education into school curricula, conducting community workshops, and leveraging media campaigns can help raise awareness and foster a culture of privacy.

Enforcement and Sanctions: Effectiveness and Deterrence

Since the enactment of the PDP Law, enforcement actions have been limited, with most cases resulting in administrative warnings rather than substantive penalties. The slow pace of legal proceedings and the lack of high-profile enforcement cases have raised questions about the law's deterrent effect.

The Role of Sanctions

Effective sanctions are essential for deterring non-compliance and signaling the seriousness of data protection obligations. The PDP Law provides for both administrative and criminal sanctions, but their impact depends on consistent and transparent enforcement. As the supervisory authority becomes operational, it will be crucial to prioritize cases that set clear precedents and demonstrate the consequences of non-compliance (Prayuti, 2024).

Alignment with International Standards

Indonesia's decision to model its PDP Law after the GDPR has several advantages. It facilitates international cooperation, enables cross-border data flows, and enhances Indonesia's credibility as a digital economy. For multinational organizations, alignment with global standards reduces compliance complexity and fosters trust in Indonesia's regulatory environment.

Local Adaptations and Contextual Challenges

Despite high alignment, the PDP Law incorporates local adaptations to reflect Indonesia's legal culture and socio-economic context. For example, certain provisions regarding consent, data subject rights, and government access to data are tailored to national priorities. Balancing these adaptations with the need for global interoperability remains an ongoing challenge.

The SME Challenge: Bridging the Compliance Gap

As highlighted in both the compliance rate chart and the results section, SMEs face unique barriers to compliance. These include:

- Resource Constraints: Limited budgets for IT upgrades, legal advice, and staff training.
- Lack of Expertise: Few SMEs have dedicated compliance or IT security personnel.
- Perceived Irrelevance: A belief that data protection is primarily an issue for large organizations or those handling sensitive data.
- Complexity of Legal Requirements: Difficulty in interpreting and implementing complex legal provisions.

Policy Recommendations for SMEs

To address these barriers, policymakers should consider:

- Simplified Guidelines: Developing sector-specific, easy-to-understand compliance checklists for SMEs.
- Technical Assistance: Providing access to government-funded or subsidized technical support.
- Incentives: Offering tax breaks or grants for SMEs that invest in data protection measures.
- Awareness Campaigns: Targeted outreach to SME associations and local business communities.

The Human Factor: Culture, Trust, and Behavioral Change

Legal mandates alone are insufficient to ensure robust data protection. Building a culture of privacy requires sustained efforts to change organizational behavior, instill ethical values, and promote accountability. Leadership commitment, employee training, and integration of privacy into business processes are critical components of this cultural shift (Gani, 2024).

Trust and Consumer Confidence

Effective data protection enhances trust between organizations and consumers. As individuals become more aware of their rights, they are likely to favor organizations that demonstrate a commitment to privacy. Conversely, high-profile breaches or incidents of non-compliance can erode consumer confidence and damage reputations.

Lessons from International Experience

The European Union's experience with the GDPR offers valuable lessons for Indonesia. Initial implementation challenges, such as compliance costs and uncertainty about enforcement, were gradually overcome through clear guidance, active supervision, and high-profile enforcement actions. Over time, the GDPR has contributed to a stronger culture of privacy and greater public awareness.

While Indonesia can draw on these lessons, contextual differences must be considered. The country's diverse socio-economic landscape, varying levels of digital literacy, and institutional capacity require tailored solutions. Nonetheless, the core principles of transparency, accountability, and rights-based protection remain universally applicable.

CONCLUSION

The implementation of Indonesia's Law No. 27 of 2022 on Personal Data Protection marks a significant advancement in the country's legal framework, aligning national policy with international standards such as the GDPR. However, empirical data and analysis reveal persistent challenges. Reported data breaches have increased exponentially since the law's enactment, as shown in the first chart, reflecting both heightened transparency and ongoing systemic vulnerabilities. Compliance rates, depicted in the second chart, demonstrate a pronounced gap between large enterprises—who are generally well-prepared—and small to medium enterprises, who struggle due to resource and knowledge constraints. Key obstacles include the delayed establishment of a supervisory authority, low public awareness, and the complexity of harmonizing the PDP Law with sectoral regulations. While the law has fostered greater awareness and accountability, its full effectiveness depends on robust enforcement, targeted support for SMEs, and sustained public education. Moving forward, Indonesia must prioritize the operationalization of its supervisory authority, enhance capacity-building initiatives, and ensure that data protection becomes an integral part of its digital transformation. Only through a holistic and inclusive approach can Indonesia realize the full promise of its personal data protection regime and safeguard the rights of all its citizens.

Acknowledgment

I would like to express my sincere gratitude to all those who contributed to the completion of this research. My heartfelt thanks go to Universitas Islam Indonesia for providing the necessary resources and support. I am especially grateful to my colleagues and experts in the field of data protection for their valuable insights and discussions. I also appreciate the contributions of stakeholders who participated in interviews and consultations. Finally, I extend my deepest thanks to my family and friends for their unwavering support and encouragement throughout this journey.

REFERENCES

Abubakar, N. S. J., Paradji, N.-S. U., Saggap, S., Anding, N. S., Tano, R. M., Arasani, A. H., Ahadain, D. R., Banda, B., Jayari, R., Alamhalil, A., Alih, S. H., & Tahil, S. K. (2024). Hacking Incidents and their Long-Term Implications for User Privacy and Trust. *Cognizance Journal of Multidisciplinary Studies, 4*(12), 443–453. https://doi.org/10.47760/cognizance.2024.v04i12.041

Adwani, A. (2025). The Evolution of Digital Payments: Implications for Financial Inclusion and Risk Management. In *Multidisciplinary Research Nexus: Ideas for the Modern World*. San International Scientific Publications. https://doi.org/10.59646/mrnc6/321

Anggraini, D. I., & Putra, P. O. H. (2025). Data Protection Impact Assessment Framework in the Banking Sector in Indonesia to Implement Law of Personal Data Protection. *Jurnal Sistem Informasi*, *21*(1), 15–34. https://doi.org/10.21609/jsi.v21i1.1439

Ehrenhard, M., Delgado, M. M., Corrales, C., & Guariento, D. (2024). Rural digital transformation: Fostering economic growth by access to services. *Open Access Government*, *44*(1), 446–447. https://doi.org/10.56367/OAG-044-11499

Gani, N. (2024). Legal Politics and Data Protection in Indonesia: A Case Study of the National Data Center Hacking. *SASI*, *30*(3), 296. https://doi.org/10.47268/sasi.v30i3.2213

Hukom, S., Humi, N., & Lukman, I. (2025). The Urgency of Legal Regulation for Personal Data Protection in Indonesia in the Big Data Era. *Hakim: Jurnal Ilmu Hukum Dan Sosial*, *3*(1), 974–992. https://doi.org/10.51903/hakim.v3i1.2291

Judijanto, L., Solapari, N., & Putra, I. (2024). An Analysis of the Gap Between Data Protection Regulations and Privacy Rights Implementation in Indonesia. *The Easta Journal Law and Human Rights*, *3*(01), 20–29. https://doi.org/10.58812/eslhr.v3i01.351

Kusuma, I. G. G. W. (2024). LAW ENFORCEMENT BY THE POLICE AGAINST JUVENILE BRAWLERS RESULTING IN FATALITIES. *Airlangga Development Journal*, *8*(2), 162–172. https://doi.org/10.20473/adj.v8i2.65119

Lihawa, R. (2025). Digital Privacy Crisis: Legal Protection of Social Media Users' Data in Indonesia's 2022 Law. *Estudiante Law Journal*, *7*(1), 280–296. https://doi.org/10.33756/eslaj.v7i1.30980

Nafaril, A. N., & Ramadhan, Y. (2024). Factors Affecting Micro Small and Medium Enterprises Taxpayer Compliance at Cilegon Pratama Tax Office. *Journal La Sociale*, *5*(2), 359–371. https://doi.org/10.37899/journal-la-sociale.v5i2.1088

Nasution, N. A. A. (2024). Peran Asosiasi Penyelenggara Jasa Internet Indonesia (APJII) Sumatera Utara dalam Mensosialisasikan Keamanan Berinternet kepada Masyarakat menurut Perspektif Komunikasi Islam. *Al-Balagh : Jurnal Komunikasi Islam*, *8*(1), 24. https://doi.org/10.37064/ab.jki.v8i1.21463

Nuzul Sa'adah, B. L., Sukarmi, S., & Dewantara, R. (2024). Establishing A Personal Data Protection Agency for E-Commerce in Indonesia. *Invest Journal of Sharia & Economic Law*, *4*(2), 292–316. https://doi.org/10.21154/invest.v4i2.10031

Omar, Z., Abdul Hamid, N., & @ Mohd Nor, F. M. (2024). A Systematic Literature Review on Government Non- Financial Assistance towards SMEs Export Performance. *International Journal of Research and Innovation in Social Science*, *VIII*(XIX), 143–152. https://doi.org/10.47772/IJRISS.2024.ICAME2411

Perdana, A., & Arifin, S. (2023). *Finding a fix for Indonesia's data protection problems* (R. Ernunsari (Ed.)). https://doi.org/10.54377/130f-dbb9

Prayuti, Y. (2024). Implications of Personal Data Protection Law in Consumer Health Data Management to Improve Secure and Confidential Handling in Indonesia. *Jurnal Ius Constituendum*, *9*(3), 461–478. https://doi.org/10.26623/jic.v9i3.9289

Sargiotis, D. (2024). Legal and Regulatory Considerations in Data Governance. In *Data Governance* (pp. 445–466). Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-67268-2_15

Triyanti, N., Handayani, I. G. A. K. R., & Karjoko, L. (2025). Legal Gaps in Personal Data Protection: Reforming Indonesia's Population Administration Law. *Hasanuddin Law Review*, *11*(1), 132. https://doi.org/10.20956/halrev.v11i1.6177

Utomo, S. (2024). Personal Data Protection Through Law Number 27 Of 2022: Challenges Of Cybercrime in The Era of Globalization and Digital. *Pena Justisia: Media Komunikasi Dan Kajian Hukum*, *23*(3), 2967–2975. https://doi.org/10.31941/pj.v23i3.5611

Zanuba, S., Saputri, M. M., & Sami'an, S. (2025). Legal Protection of Persons with Mental Disorders in Health Services in Accordance with Laws and Regulations in Indonesia. *Jurnal Hukum Indonesia*, *4*(2), 86–94. https://doi.org/10.58344/jhi.v4i2.1615

Zuwanda, Z. S., Judijanto, L., Khuan, H., & Triyantoro, A. (2024). Normative Study of Law No. 27 of 2022 on the Protection of Personal Data and its Impact on the Fintech Industry in Indonesia. *West Science Law and Human Rights*, *2*(04), 421–428. https://doi.org/10.58812/wslhr.v2i04.1367