Journal of Cyber Law and Information Security
Volume 2, Number 1, 2023

Understanding Data Controller Responsibilities under Indonesia's PDP Law: Legal Challenges in Ensuring Compliance

Cindi Mutia[1*]

[1] Universitas Sarjanawiyata Tamansiswa, Yogyakarta, Indonesia

Abstract

Article history:
Received: January 13, 2023
Revised: February 11, 2023
Accepted: March 22, 2023
Published: June 30, 2023

Keywords:
Accountability, Compliance, Data Controller, Information Security, Personal Data Protection.

Identifier:
Zera Open
Page: 21-39
https://zeraopen.com/journal/jclis

This article examines data controller responsibilities under Indonesia's Law Number 27 of 2022 concerning Personal Data Protection within the broader context of cyber law and information security governance. The discussion is guided by two questions: how effective is the PDP Law in regulating data controller responsibilities in Indonesia, and why is controller compliance urgent for Indonesia's digital legal framework? This study plays a role in clarifying the legal position of data controllers as the main actors responsible for determining the purposes and control of personal data processing. Using a normative legal approach, the article analyzes statutory provisions, legal principles, scholarly literature, and selected data breach cases as contextual support. The results show that the PDP Law has strengthened Indonesia's personal data protection framework by establishing clearer controller obligations, including lawful processing, transparency, security, breach notification, and respect for data subject rights. However, its effectiveness remains limited by challenges in technical implementation, institutional supervision, enforcement consistency, and organizational compliance readiness. The article finds that controller accountability must be transformed from statutory duty into measurable compliance practice.

*Corresponding author:
(Cindi Mutia)

1. Introduction

Personal data protection has become a central issue in cyber law because digital services increasingly depend on the collection, storage, analysis, transfer, and monetization of personal information. In Indonesia, this issue is particularly important because public and private institutions process personal data in e-commerce, financial technology, health care, education, public administration, telecommunications, and social media services. Earlier studies have shown that Indonesia's personal data protection framework was previously fragmented across sectoral regulations, creating uncertainty regarding consent, security standards, institutional supervision, and remedies for data subjects (Rosadi, 2018; Sautunnida, 2018). The enactment of Law Number 27 of 2022 concerning Personal Data Protection, commonly known as the PDP Law, therefore represents a major legal development because it introduces a more comprehensive framework for regulating the rights of data subjects and the obligations of parties that process personal data.

The urgency of this legal development is also shaped by repeated data breach incidents. The Tokopedia case, for example, attracted public attention after allegations emerged that millions of user records had been leaked and circulated online (Potkin, 2020). A similar concern appeared in the BPJS Kesehatan case, where Indonesian authorities investigated an alleged personal data breach involving the national health insurance system (Reuters, 2021). These incidents show that personal data protection is not merely a matter of individual privacy, but also a question of digital trust, consumer protection, institutional accountability, and national information security. As Marune and Hartanto (2021) argue, strengthening personal

data protection must be connected with cybersecurity readiness and public awareness, since legal norms will be ineffective if they are not supported by preventive governance and institutional capacity.

Within the PDP Law, the concept of the personal data controller is especially important. A controller determines the purposes and exercises control over personal data processing, which means that its legal position is not passive or merely administrative. Instead, the controller carries core responsibilities related to lawful processing, transparency, accuracy, security, confidentiality, breach notification, impact assessment, and respect for data subject rights. Yuniarti (2022) notes that the PDP Law strengthens the recognition of data protection after years of regulatory uncertainty. However, the existence of statutory obligations does not automatically ensure compliance. The main challenge lies in translating legal duties into operational standards, internal governance systems, documentation practices, audit mechanisms, and enforceable accountability.

Several scholarly discussions have emphasized that Indonesia's personal data protection framework must address both normative and practical weaknesses. Attidhira and Permana (2022) highlight the need for a clearer legal framework and stronger mechanisms to protect personal data. Lestari and Mujib (2022) similarly argue that a comprehensive framework requires effective oversight and harmonization with established personal data protection principles. In the context of digital transactions, Setiawan et al. (2020) show that consumer personal data protection remains vulnerable when business actors lack clear obligations or when enforcement is weak. These findings indicate that controller responsibility should be

studied not only as a textual obligation in the PDP Law, but also as a compliance problem involving legal interpretation, institutional supervision, and organizational readiness.

This article therefore focuses on the responsibilities of data controllers under Indonesia's PDP Law and the legal challenges in ensuring compliance. The study is important because the controller is the main legal actor responsible for determining why and how personal data is processed. If controller obligations are unclear, inconsistently implemented, or weakly supervised, the protection promised by the PDP Law may remain formal rather than effective. Based on this problem, the article addresses two research questions: how effective is the PDP Law in regulating data controller responsibilities in Indonesia, and why is the regulation of data controller compliance urgent for Indonesia's cyber law and information security framework? By using a normative legal approach, the article examines statutory provisions, legal principles, and relevant scholarly arguments to assess the effectiveness and urgency of controller responsibility as a key element of personal data protection governance.

2. Research Methods

This study uses a normative legal research method to examine data controller responsibilities under Law Number 27 of 2022 concerning Personal Data Protection. A normative approach is appropriate because the article focuses on legal norms, statutory obligations, regulatory coherence, and the extent to which the PDP Law provides an effective basis for ensuring controller compliance. The research does not measure compliance through field data, interviews, or surveys, but analyzes

the legal framework governing personal data processing and the responsibilities imposed on personal data controllers in Indonesia.

The primary legal material used in this study is Law Number 27 of 2022 concerning Personal Data Protection. This law is examined as the central regulation because it introduces specific provisions on personal data subjects, personal data controllers, personal data processors, lawful processing, consent, breach notification, sanctions, and institutional supervision. The study also refers to related Indonesian cyber law instruments where relevant, particularly regulations concerning electronic systems, digital transactions, and electronic system operators. These related regulations are used to understand how the PDP Law interacts with the broader Indonesian cyber law framework.

Secondary legal materials consist of peer-reviewed journal articles, scholarly discussions, and academic legal analyses concerning personal data protection, privacy rights, digital governance, cybersecurity, consumer protection, and data breach accountability in Indonesia. The literature was selected based on relevance to the article's focus, publication credibility, and its contribution to explaining regulatory effectiveness or compliance challenges. News reports from reputable media are used only as supporting contextual materials to illustrate real data breach cases and the urgency of strengthening controller responsibility. They are not treated as the main legal basis of analysis.

The research applies statutory, conceptual, and analytical approaches. The statutory approach is used to examine the provisions of the PDP Law and related cyber regulations. The conceptual approach is used to clarify key legal concepts,

especially personal data controller, personal data subject, consent, accountability, compliance, and legal responsibility. The analytical approach is used to evaluate whether the PDP Law provides sufficient clarity, enforceability, and institutional support for regulating controller obligations.

The analysis is conducted qualitatively through legal interpretation and systematic comparison between legal provisions and compliance needs in digital data processing. The study first identifies the duties imposed on data controllers, then evaluates their effectiveness in addressing compliance problems. It further analyzes why controller responsibility is urgent for Indonesia's cyber law and information security framework. Through this method, the article aims to provide a structured normative assessment of the PDP Law as both a privacy regulation and a compliance instrument.

3. Results and Discussion

3.1. How Effective Is the PDP Law in Regulating Data Controller Responsibilities in Indonesia?

The enactment of Law Number 27 of 2022 concerning Personal Data Protection marks an important shift in Indonesia's cyber law framework because it moves personal data protection from a fragmented sectoral arrangement toward a more unified statutory model. Before the PDP Law, personal data protection was regulated through scattered provisions in electronic information, telecommunications, population administration, banking, health, and consumer protection regulations. This created uncertainty because different sectors applied

different standards, while many digital activities involved cross-sectoral data processing. Rosadi (2018) explains that Indonesia's earlier privacy protection framework had not yet provided comprehensive safeguards for personal data in the digital economy. Sautunnida (2018) also emphasizes that the absence of a specific personal data protection law created legal uncertainty, especially when compared with countries that had already developed more structured privacy frameworks. In this context, the PDP Law is effective at the normative level because it establishes a clearer legal foundation for identifying who is responsible for personal data processing and what obligations must be fulfilled.

One of the main strengths of the PDP Law is its recognition of the personal data controller as a central legal actor. The controller is not merely a party that stores data, but a party that determines the purposes and controls the processing of personal data. This definition is important because liability in digital ecosystems should not only be attached to technical operators, but also to institutions that decide why data is collected, how it is used, who may access it, and how long it will be retained. By placing controllers at the center of responsibility, the PDP Law strengthens the accountability principle. This is consistent with the view of Yuniarti (2022), who argues that the PDP Law strengthens legal recognition of personal data protection after a long period of regulatory uncertainty. Therefore, the law is effective in establishing a more definite legal subject for compliance, especially compared with the previous framework that often relied on the broader concept of electronic system operators.

The PDP Law also regulates several substantive obligations that are relevant to controller responsibility. These include the obligation to process personal data based on lawful grounds, obtain valid consent where required, ensure transparency, maintain data accuracy, protect confidentiality, prevent unlawful access, respond to data subject requests, and notify relevant parties in the event of a personal data breach. These obligations are significant because they transform personal data protection from a passive privacy claim into an active compliance duty. In other words, the controller must build internal mechanisms before violations occur, not merely respond after harm has already happened. This reflects a preventive model of legal responsibility. Fauzi and Shandy (2022) explain that the PDP Law is connected to the legal politics of privacy protection, meaning that the law should be understood as part of the state's effort to guarantee privacy as a constitutional and human rights interest. From this perspective, controller responsibility is not only a matter of administrative compliance, but also a legal mechanism to protect individual autonomy and dignity in digital spaces.

However, the effectiveness of the PDP Law remains limited by several legal and practical challenges. The first challenge concerns the clarity of implementation. Although the law provides general obligations, many of those obligations require further technical interpretation. For example, controllers must ensure personal data security, but the law does not fully specify detailed sectoral standards for encryption, access control, data minimization, retention schedules, vendor assessment, or privacy impact assessment procedures. This creates a gap between legal norms and operational compliance. A large corporation may have the resources to develop

internal data governance systems, but small and medium-sized enterprises may struggle to interpret what minimum compliance requires. As Attidhira and Permana (2022) argue, Indonesia still needs stronger mechanisms and clearer legal arrangements to make personal data protection more effective. Without detailed guidance, controllers may comply only formally by preparing consent forms or privacy policies, while failing to build substantive safeguards.

The second challenge concerns supervision and enforcement. A law can be normatively strong but practically weak if supervision is delayed, fragmented, or inconsistent. The PDP Law requires institutional mechanisms to ensure that controllers comply with their obligations, but the effectiveness of those obligations depends heavily on the capacity of supervisory authorities to issue guidance, receive complaints, conduct investigations, impose sanctions, and coordinate with sectoral regulators. Lestari and Mujib (2022) emphasize that an effective personal data protection framework requires oversight and harmonization with established data protection principles. This is especially important because personal data processing occurs across many sectors, including finance, telecommunications, health, e-commerce, education, and public services. If supervisory authority is unclear or weak, controllers may treat compliance as a low-risk obligation rather than a binding legal duty.

The third challenge concerns enforcement culture. Indonesian digital governance has often relied on reactive responses after data breaches occur. The Tokopedia and BPJS Kesehatan cases show how data breach incidents can create public concern, reputational harm, and distrust in digital services (Potkin, 2020;

Reuters, 2021). These cases illustrate why controller responsibility must be measured not only by whether a law exists, but also by whether the law changes institutional behavior. Setiawan et al. (2020) show that consumer personal data remains vulnerable in digital transactions when business actors are not clearly controlled or when enforcement is weak. This means that the PDP Law will be effective only if controllers are encouraged, supervised, and compelled to adopt compliance systems before violations happen.

The fourth challenge concerns the relationship between controller responsibility and processor responsibility. In practice, many controllers rely on third-party service providers, cloud storage vendors, payment gateways, analytics companies, and outsourced technology providers. This makes personal data processing more complex because data may move through multiple actors. The PDP Law distinguishes controllers and processors, but compliance risks remain when contracts, instructions, security standards, and audit rights are not clearly arranged. A controller may claim that a breach occurred through a processor, while a processor may claim that it only followed the controller's instructions. Therefore, effective controller responsibility requires clear contractual governance, due diligence, and continuing monitoring of processors. Simbolon and Juwono (2022) note that Indonesia's PDP Law shares several similarities with the EU GDPR regarding data subject rights, but the effectiveness of such rights depends on implementation and institutional support. This comparison shows that legal borrowing from stronger regulatory models must be accompanied by domestic enforcement capacity.

Overall, the PDP Law is effective in establishing the normative foundation of data controller responsibility, but its practical effectiveness remains conditional. It successfully identifies controllers as accountable legal actors, introduces rights and obligations, and provides a basis for sanctions. However, it still faces challenges in technical implementation, supervisory readiness, compliance culture, and coordination across sectors. Therefore, the law should be seen as an important starting point rather than a complete solution. Its effectiveness will depend on implementing regulations, institutional enforcement, sectoral guidance, organizational awareness, and the willingness of controllers to treat personal data protection as a core governance obligation.

3.2. Why Is the Regulation of Data Controller Compliance Urgent for Indonesia's Cyber Law and Information Security Framework?

The regulation of data controller compliance is urgent because personal data has become a strategic asset in Indonesia's digital economy. Digital platforms, financial technology services, online marketplaces, public applications, health systems, and educational platforms rely on personal data to identify users, personalize services, assess risk, process transactions, and make automated decisions. This creates benefits for efficiency and innovation, but it also creates serious legal risks when data is collected excessively, processed without transparency, transferred without control, or stored without adequate security. Lesmana et al. (2021) argue that personal data protection is urgent because it is closely related to the fulfillment of the right to privacy. This means that controller compliance is not

merely a technical matter, but a legal necessity to ensure that digital transformation does not weaken fundamental rights.

The urgency is also connected to the increasing scale and impact of data breach incidents. When personal data is leaked, the harm is not limited to the immediate exposure of names, telephone numbers, email addresses, identification numbers, or addresses. The leaked data can be used for fraud, phishing, identity theft, illegal profiling, doxing, financial manipulation, and social engineering. In some sectors, such as health and finance, the harm can be more serious because the data may reveal sensitive personal conditions or economic vulnerabilities. Marune and Hartanto (2021) emphasize that personal data protection must be strengthened together with cybersecurity and public awareness. This is important because legal protection will be incomplete if controllers do not develop preventive security systems and if data subjects do not understand their rights.

From a cyber law perspective, controller compliance is urgent because the PDP Law must function as a bridge between privacy protection and information security governance. Privacy protection focuses on the rights of individuals over their personal data, while information security focuses on protecting information from unauthorized access, alteration, destruction, or disclosure. These two objectives are closely connected. A controller cannot respect privacy rights if it does not maintain information security, and security measures will lack legal direction if they are not connected to data subject rights and lawful processing principles. The PDP Law provides this bridge by requiring controllers to process personal data lawfully and securely. However, the bridge will only work if controllers develop

internal compliance systems, including data inventories, consent management, access restrictions, breach response procedures, retention policies, staff training, and vendor governance.

The regulation of controller compliance is also urgent because Indonesia's digital ecosystem involves both public and private controllers. Public institutions process population, health, education, taxation, social assistance, and administrative data. Private entities process consumer, transaction, location, behavioral, biometric, and financial data. Both categories can create serious risks when compliance is weak. In public institutions, weak compliance can reduce public trust in government digital services. In private institutions, weak compliance can harm consumers and reduce confidence in digital commerce. Kusnadi (2021) explains that personal data protection is part of the legal protection of privacy rights, while Setiawan et al. (2020) show that consumer data in e-commerce transactions requires stronger protection. These arguments show that controller compliance is needed across both governance and market contexts.

Another reason why controller compliance is urgent is that consent alone is not sufficient to protect data subjects. Many digital services rely on long privacy policies and standard-form consent mechanisms that users rarely read or fully understand. If the law places too much emphasis on consent without requiring controller accountability, the burden of protection shifts unfairly to individuals. Data subjects may click "agree" because they need access to a service, not because they have meaningful bargaining power. Therefore, controller responsibility must include transparency, proportionality, purpose limitation, security safeguards, and

accountability. The controller must be required to justify why data is collected and how it is protected. This approach is consistent with modern personal data protection principles, where consent is only one legal basis among broader obligations.

The urgency of controller compliance is also related to legal certainty for business actors. Some may view the PDP Law as a regulatory burden, but clear compliance standards can actually support responsible innovation. When businesses understand what data they may collect, how they must store it, when they must delete it, and how they must respond to data subject requests, they can design safer and more trustworthy digital services. Legal certainty also reduces the risk of disputes, sanctions, reputational damage, and consumer distrust. Simbolon and Juwono (2022) show that Indonesia's PDP framework has similarities with the EU GDPR, especially regarding data subject rights. This indicates that Indonesia is moving toward global data protection standards, which may also support cross-border trust and international digital cooperation.

Nevertheless, urgency does not mean that regulation should only focus on punishment. Sanctions are important, but compliance requires a broader regulatory ecosystem. Controllers need clear guidance, sector-specific standards, practical compliance tools, awareness programs, and predictable enforcement. Supervisory institutions must be independent, capable, and accessible. Data subjects must be able to exercise their rights without excessive procedural barriers. Courts and enforcement bodies must also develop a consistent interpretation of controller

responsibility. Without these supporting elements, the PDP Law may become a formal legal instrument that is difficult to apply consistently.

Therefore, the regulation of data controller compliance is urgent because it determines whether the PDP Law can operate as an effective cyber law instrument. The law's promise of personal data protection depends on the behavior of controllers as the main actors that determine the purposes and means of processing. If controllers are not regulated effectively, data subjects remain vulnerable despite the existence of statutory rights. If controllers are regulated clearly and supervised properly, the PDP Law can strengthen privacy protection, digital trust, consumer protection, cybersecurity governance, and legal certainty. For Indonesia, this is especially important because digital transformation continues to expand faster than public understanding and institutional readiness. Controller compliance must therefore be treated as a central priority in the development of Indonesia's personal data protection regime.

4. Conclusion

This article concludes that Law Number 27 of 2022 concerning Personal Data Protection has created a stronger normative foundation for regulating data controller responsibilities in Indonesia. The PDP Law is important because it identifies the personal data controller as the main legal actor responsible for determining the purposes and control of personal data processing. Through this position, the controller is required to ensure lawful processing, transparency, data accuracy, confidentiality, security, breach notification, and respect for data subject rights.

Compared with the previous fragmented regulatory framework, the PDP Law provides a more comprehensive basis for accountability. It also strengthens the legal recognition of personal data protection as part of privacy rights, consumer protection, cybersecurity governance, and digital trust. Therefore, at the normative level, the PDP Law can be considered effective in clarifying the basic responsibilities of data controllers.

However, the effectiveness of the PDP Law remains limited by several implementation challenges. Many controller obligations still require clearer technical standards, sectoral guidance, and practical compliance mechanisms. Legal provisions on security, consent, breach response, documentation, and accountability will be difficult to enforce if controllers do not understand how to translate them into internal policies and operational procedures. The effectiveness of the law also depends on institutional supervision, enforcement consistency, and coordination between the personal data protection authority and sectoral regulators. Without strong oversight, controller responsibility may remain formal rather than substantive. Data controllers may comply only by preparing privacy notices or consent forms, while failing to develop real safeguards such as data inventories, access control, retention policies, staff training, vendor management, and breach response systems.

The regulation of data controller compliance is urgent because Indonesia's digital transformation continues to increase the volume, value, and sensitivity of personal data processed by public and private institutions. Data breach cases show that weak personal data governance can harm individuals, reduce public trust, and

threaten information security. For that reason, the PDP Law should not be understood only as a privacy statute, but also as a key instrument of cyber law and information security governance. To strengthen its effectiveness, Indonesia needs implementing regulations, practical compliance guidelines, stronger supervisory institutions, predictable enforcement, and broader awareness among controllers and data subjects. The main finding of this article is that the PDP Law has established an essential legal foundation, but its success depends on whether controller accountability can be transformed from statutory obligation into measurable compliance practice. Thus, data controller responsibility must become a central priority in the development of Indonesia's personal data protection regime.

References

Attidhira, S. W., & Permana, Y. S. (2022). Review of personal data protection legal regulations in Indonesia. *Awang Long Law Review, 5*(1), 280–294.

Fauzi, E., & Shandy, N. A. R. (2022). Hak atas privasi dan politik hukum Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi. *Lex Renaissance, 7*(3), 445–461.

Kusnadi, S. A. (2021). Perlindungan hukum data pribadi sebagai hak privasi. *AL WASATH Jurnal Ilmu Hukum, 2*(1), 9–16.

Lesmana, C. S. A. T., Elis, E., & Hamimah, S. (2021). Urgensi Undang-Undang Perlindungan Data Pribadi dalam menjamin keamanan data pribadi sebagai pemenuhan hak atas privasi masyarakat Indonesia. *Jurnal Rechten: Riset Hukum dan Hak Asasi Manusia, 3*(2), 1–6.

Lestari, Y., & Mujib, M. M. (2022). Optimizing personal data protection legal framework in Indonesia. *Supremasi Hukum, 11*(2), 205–234.

Marune, A. E. M. S., & Hartanto, B. (2021). Strengthening personal data protection, cyber security, and improving public awareness in Indonesia: Progressive legal perspective. *International Journal of Business, Economics and Social Development, 2*(4), 143–152.

Potkin, F. (2020, May 2). Indonesia's Tokopedia probes alleged data leak of 91 million users. *Reuters*. Retrieved Jan 11, 2023 from https://www.reuters.com/article/technology/indonesias-tokopedia-probes-alleged-data-leak-of-91-million-users-idUSKBN22E0P9/

Republic of Indonesia. (2022). *Law Number 27 of 2022 concerning Personal Data Protection*. https://peraturan.bpk.go.id/Details/229798/uu-no-27-tahun-2022

Reuters. (2021, May 21). Indonesia summons state health insurer over alleged data leak. *Reuters*. Retrieved Jan 14, 2023 from https://www.reuters.com/technology/indonesia-summons-state-health-insurer-over-alleged-data-leak-2021-05-21/

Rosadi, S. D. (2018). Protecting privacy on personal data in digital economic era: Legal framework in Indonesia. *Brawijaya Law Journal, 5*(1), 143–157.

Sautunnida, L. (2018). Urgensi Undang-Undang Perlindungan Data Pribadi di Indonesia: Studi perbandingan hukum Inggris dan Malaysia. *Kanun Jurnal Ilmu Hukum, 20*(2), 369–384.

Setiawan, H., Ghufron, M., & Mochtar, D. A. (2020). Perlindungan hukum terhadap data pribadi konsumen dalam transaksi e-commerce. *MLJ Merdeka Law Journal, 1*(2), 102–111.

Simbolon, V. A., & Juwono, V. (2022). Comparative review of personal data protection policy in Indonesia and the European Union General Data Protection Regulation. *Publik: Jurnal Ilmu Administrasi, 11*(2), 178–190.

Yuniarti, S. (2022). Protection of Indonesia's personal data after ratification of Personal Data Protection Act. *Progressive Law Review, 4*(2), 54–68.