

Legal Protection of Personal Data in Indonesia Following the Enactment of Law No. 27 of 2022 on Personal Data Protection

Michelle Nabila Andaista Bangsu ^{1*} Dicky Ega Brahmento ² Alia Shifa ³

^{1*, 2, 3} Faculty of Law, Universitas Trisakti, Jakarta, Indonesia

Email: bangsumichelle@gmail.com

ARTICLE HISTORY

Submitted : June 30, 2026
Reviewed : July 10, 2026
 : July 16, 2026
Revised : July 18, 2026
Accepted : July 19, 2026
Published : August 11, 2026

Conflict of Interest Statement:

The author(s) declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

ABSTRACT

Purpose: This study aims to analyze the legal framework for personal data protection in Indonesia following the enactment of Law No. 27 of 2022 on Personal Data Protection (PDP Law), as well as to identify the normative challenges in its implementation.

Research Method: This study employs a normative legal methodology with legislative, conceptual, and comparative approaches through qualitative analysis of primary and secondary legal sources.

Results and Discussion: The research findings indicate that the Personal Data Protection Act (PDP Act) has established a more comprehensive legal framework through provisions governing the rights of data subjects, the obligations of data controllers and processors, the principles of personal data processing, and mechanisms for administrative and criminal accountability. However, its implementation still requires harmonization with sector-specific regulations, strengthening supervisory institutions, refining regulations regarding AI-based data processing, profiling, and cross-border data transfers, as well as strengthening law enforcement mechanisms.

Implications: These findings serve as the basis for refining policies and regulations that implement personal data protection in Indonesia.

Originality: The novelty of this research lies in its doctrinal analysis, which integrates the normative framework of the Personal Data Protection Act, the harmonization of sector-specific regulations, and a comparative perspective with the GDPR.

Keywords: personal data protection; right to privacy; legal harmonization; GDPR; processing of personal data.

1. Introduction

Advances in information and communication technology have brought about significant changes in various aspects of people's lives. The increasing use of the internet, social media, digital banking services, e-commerce, digital health services, and e-government systems demonstrates that digital transformation has become an integral part of social and economic activities. In each of these activities, personal data serves as a legal identifier and is used for identification, authentication, verification, and the provision of digital services. Consequently, the collection, storage, use, disclosure, and processing



of personal data occur on a massive scale, thereby increasing the risk of data breaches, unauthorized access, misuse, or the use of data beyond legitimate purposes. These conditions have the potential to cause material and immaterial harm to data subjects and heighten the need for effective legal protection of personal data (Manurung & Thalib, 2023)

Personal data is, by its very nature, an integral part of the right to privacy, which is recognized as a human right. In Indonesia, the constitutional guarantee of this right is enshrined in Article 28G(1) of the 1945 Constitution of the Republic of Indonesia, which protects the person, family, honor, dignity, and property of every citizen. From a legal perspective, the protection of personal data is a manifestation of the state's obligation to ensure respect for, protection of, and fulfillment of citizens' constitutional rights in the digital realm. Therefore, establishing legal instruments governing the rights of data subjects, the obligations of personal data controllers, and law enforcement mechanisms is a crucial part of efforts to achieve legal certainty and protect privacy rights (Fauzy & Shandy, 2023).

Following the enactment of No. 27 of 2022 on Personal Data Protection (PDP Law), regulations concerning personal data no longer rely solely on various sectoral provisions, such as Law No. 11 of 2008 on Electronic Information and Transactions and its amendments, as well as Government Regulation No. 71 of 2019 on the Implementation of Electronic Systems and Transactions. Although the PDP Act serves as a *lex specialis* in the protection of personal data, its implementation continues to interact with various sectoral regulations, thereby raising issues regarding the harmonization of norms, the division of authority among agencies, and law enforcement mechanisms for resolving personal data breaches. This situation indicates that the issue of personal data protection is not only related to the existence of legal norms but also to the consistency of the legal system in integrating the various provisions governing the processing of personal data in Indonesia.

Studies on personal data protection in Indonesia following the enactment of Law No. 27 of 2022 have evolved into several key themes. The research by Fauzy and Shandy (2023) focuses on the relationship between the constitutional right to privacy and the legal policies underpinning the enactment of the Personal Data Protection Law (PDP Law). It emphasizes that personal data protection is a legal consequence of advancements in information and communication technology. In line with this, Fauzy and Shandy (2023) explain that the state has an obligation to guarantee the protection of the right to privacy through the establishment of legal instruments that provide legal certainty for data subjects. These studies provide a conceptual foundation regarding the constitutional legitimacy of personal data protection; however, their analysis remains focused on the normative justification for the enactment of the Personal Data Protection Act (PDP Act) without delving deeply into the relationship between the provisions of the PDP Act and sectoral regulations or its law enforcement mechanisms. Other research indicates that the Personal Data Protection Act (PDP Act) has provided preventive protection mechanisms through provisions on data subjects' rights, data controllers' obligations, and principles of personal data processing, as well as repressive protection through the imposition of administrative and criminal sanctions for personal data violations (Kurdi & Cahyono, 2024; Putri *et al.*, 2024).

Recent research developments have shifted toward discussions on the implementation of the PDP Act following its enactment. Bachtiar *et al.*, (2025) found that the effectiveness of PDP Act implementation remains influenced by regulatory ambiguities regarding certain normative aspects, as well as suboptimal institutional oversight mechanisms. These findings are reinforced by Hukom *et al.*, (2025), who reported that organizations' compliance with personal data protection obligations remains suboptimal, while Kurdi & Cahyono (2024) highlighted the lack of an independent supervisory body as

one of the obstacles to the implementation of the PDP Act. Furthermore, Rinjani & Firmansyah (2025) indicate that implementation challenges are also influenced by the readiness of institutions to meet data protection standards as well as the increasingly complex development of digital technology. Nevertheless, most of these studies still frame the implementation of the Personal Data Protection Act as an issue of administrative compliance or policy effectiveness, thus failing to provide an in-depth legal analysis regarding the interpretation of legal norms, the interrelationships among regulations, the scope of institutional authority, or the alignment of the Act's legal framework with international data protection regimes such as the General Data Protection Regulation (GDPR).

Although various studies have confirmed that Law No. 27 of 2022 establishes a relatively comprehensive framework for personal data protection and identifies several implementation challenges, these conclusions have become commonplace in the literature. Most studies remain focused on describing the substance of the Personal Data Protection Act or providing a general evaluation of the effectiveness of its implementation; consequently, they have not yet offered a systematic legal analysis examining the relationship between the provisions of the Personal Data Protection Act and sector-specific regulations, the scope of authority of the relevant agencies, legal protection mechanisms for data subjects, or potential conflicts of law in enforcement practice. Consequently, contributions to the development of the legal doctrine of personal data protection remain relatively limited, as discussions have not yet delved deeply into interpreting statutory provisions.

Furthermore, advancements in digital technology, cross-border data processing, the use of artificial intelligence, profiling, and automated decision-making raise new legal issues that have not yet been extensively analyzed in the context of the Personal Data Protection Act. However, these issues are directly related to the legality of personal data processing, the principles of accountability and transparency, data protection impact assessments (data protection impact assessment), data breach notifications (data breach notification), and mechanisms for transferring personal data outside Indonesia. The limited research on these aspects highlights the need for a normative legal analysis that not only systematically interprets the provisions of the Personal Data Protection Act but also compares them with international standards—particularly the General Data Protection Regulation (GDPR)—to assess the consistency of Indonesia's legal framework for personal data protection.

Based on this research gap, this study aims to answer two main questions: (1) what is the legal framework for personal data protection in Indonesia following the enactment of Law No. 27 of 2022 on Personal Data Protection; and (2) what are the implementation challenges and prospects for the development of personal data protection within the Indonesian legal system based on an analysis of applicable legal norms. In line with these questions, this study aims to conduct a doctrinal analysis of the forms of legal protection stipulated in the Personal Data Protection Act (PDP Act), interpret the relationship between its provisions and sectoral regulations, and evaluate the challenges of its implementation through legislative, conceptual, and comparative approaches.

The novelty of this study lies in the analytical approach employed. Unlike previous studies, which generally focused on describing legal norms or evaluating implementation in general, this study develops a doctrinal legal analysis of the relationship between the Personal Data Protection Act and sectoral regulations, the interpretation of data subjects' rights and data controllers' obligations based on statutory provisions, the scope of institutional authority in enforcing personal data protection laws, as well as a systematic comparison with the General Data Protection Regulation (GDPR) regarding the legal basis for data processing (lawful basis), scope of application (extraterritorial application), automated processing (automated processing), data breach notification (breach notification), cross-

border data transfers (cross-border data transfer), and enforcement mechanisms (enforcement mechanisms). Thus, this study is expected to contribute to the development of the legal doctrine of personal data protection while strengthening the harmonization of the Indonesian legal system with developments in the international personal data protection regime.

The remainder of this paper is organized as follows. Section 2 provides a literature review and hypothesis development. Section 3 presents the research method and design. Section 4 provides the results and discussion. Section 5 is Concluding Remarks and Recommendations.

2. Literature Review and Hypothesis Development

2.1 *The Concept of Personal Data Protection as a Constitutional Right and a Human Right*

The protection of personal data is a manifestation of the right to privacy, which has evolved into one of the fundamental rights in modern legal systems and is recognized as part of human rights. In the context of the rule of law, the right to privacy encompasses not only the protection of an individual's private life but also the individual's authority to control the collection, use, storage, disclosure, and processing of their personal data. In Indonesia, the constitutional guarantee of this right is reflected in Article 28G(1) of the 1945 Constitution of the Republic of Indonesia, which protects the person, family, honor, dignity, and sense of security of every citizen. Therefore, personal data protection is a legal consequence of the recognition of these constitutional rights and simultaneously constitutes the state's obligation to ensure respect for, protection of, and fulfillment of citizens' rights in the digital sphere (Fauzy & Nabila Alif Radika Shandy, 2023; Manurung & Thalib, 2023). In line with developments in international law, the right to personal data protection is also viewed as part of the human rights framework, deriving its legitimacy from various international instruments, such as the Universal Declaration of Human Rights (UDHR), the International Covenant on Civil and Political Rights (ICCPR), and the data protection principles established in the European Union's General Data Protection Regulation (GDPR). Thus, personal data protection is no longer understood merely as a technical issue of information security, but rather as a legal instrument that guarantees individual autonomy, legal certainty, and respect for human dignity in a digital society (Palit & Purba, 2025; Ravinka & Widiatedja, 2022).

From a national legal perspective, recognizing personal data protection as a constitutional right serves as the foundation for the enactment of Law No. 27 of 2022 on Personal Data Protection (PDP Law). This law affirms that all processing of personal data must be conducted in accordance with the principles of legality, legitimate purpose, transparency, accountability, purpose limitation, and protection of the data subject's rights. These provisions reflect a paradigm shift from data protection—previously scattered across various sectoral regulations—toward a more comprehensive and integrated legal framework. Personal data protection is intended not only to safeguard individual interests but also to maintain a balance between the use of digital technology, economic interests, and the protection of human rights in the operation of electronic systems (Widodo *et al.*, 2024). However, the effectiveness of such rights protection is determined not only by the existence of legal norms but also by regulatory harmonization, clarity regarding institutional authority, and consistency in practical implementation. Therefore, personal data protection must be understood as a legal regime that comprehensively integrates constitutional, human rights, and data processing governance dimensions so that it can provide legal certainty while addressing the challenges posed by the development of digital technology (Judijanto *et al.*, 2024; M. A. Nirwana, 2022).

2.2 The Legal Framework for Personal Data Protection in Law No. 27 of 2022

Law No. 27 of 2022 on Personal Data Protection (PDP Law) is a *lex specialis* that establishes a comprehensive legal framework for personal data protection in Indonesia. Unlike previous regulations, which were scattered across various sectoral laws, the PDP Law integrates the definition of personal data, the classification of specific and general personal data, the rights of data subjects, the obligations of data controllers and processors, data processing mechanisms, cross-border data transfers, dispute resolution, as well as administrative and criminal sanctions into a single, cohesive legal framework. This structure reflects a paradigm shift from a sectoral approach toward a rights-based data protection system (rights-based approach), positioning data subjects as rights holders who have control over the processing of their personal data (Budiarta *et al.*, 2023). From a normative perspective, the PDP Act not only recognizes the rights of data subjects—such as the right to obtain information, the right to access, rectify, erase, and restrict the processing of personal data—but also imposes legal obligations on data controllers to apply the principles of legality, transparency, accountability, purpose limitation, security of processing, and protection of data confidentiality. Thus, the legal framework of the PDP Act is designed to ensure legal certainty while striking a balance between the interests of data utilization and the protection of citizens' privacy rights (Firdaus, 2024; Putri *et al.*, 2024).

Although the PDP Act has normatively established a more systematic protection framework, the effectiveness of its legal framework depends heavily on harmonization with sectoral regulations, institutional certainty, and consistency in law enforcement. One concern remains the suboptimal institutional framework for an independent supervisory authority, even though such an authority plays a crucial role in ensuring compliance by data controllers, resolving disputes, and overseeing cross-border transfers of personal data (Ayiliani & Farida, 2024). Furthermore, the protection of personal data is not only the responsibility of data controllers but also a constitutional obligation of the state to provide an effective legal system to prevent the misuse of personal data and protect citizens' rights in the digital space (Aqilah *et al.*, 2022). Therefore, implementing the Personal Data Protection Act (PDP Act) requires harmonization with other regulations, including amendments to the Electronic Information and Transactions Act, to avoid overlapping norms or legal uncertainty in practice (Abita *et al.*, 2024). From a human rights perspective, this legal framework must also ensure that all personal data processing is carried out lawfully, proportionally, and accountably, so that personal data protection is not merely an administrative obligation but also an instrument for safeguarding citizens' constitutional rights (K & Makkawaru, 2024).

2.3 Harmonization of the Personal Data Protection Act with Sectoral Regulations and Implementation Challenges

Law No. 27 of 2022 on Personal Data Protection (PDP Law) was designed as a *lex specialis* that serves as the primary legal framework for personal data protection in Indonesia. However, its implementation cannot be separated from various sectoral regulations that have previously governed aspects of data processing, such as the Law on Electronic Information and Transactions, Government Regulation No. 71 of 2019 on the Operation of Electronic Systems and Transactions, as well as regulations in the financial, health, and government administration sectors. This situation creates a need for regulatory harmonization to prevent overlapping jurisdictions, differing protection standards, and legal uncertainty in the operation of electronic systems. Regulatory harmonization aims not only to ensure consistency among regulations but also to guarantee that all data controllers across various sectors uniformly apply

the principles of personal data protection. In practice, gaps still exist between normative regulations and the implementation of privacy rights protection due to a lack of policy synchronization among institutions, differences in oversight mechanisms, and suboptimal coordination within the national cybersecurity system (Given this suboptimal coordination, the effectiveness of the Personal Data Protection Act (PDP Act) requires the integration of data protection policies with national cybersecurity governance through more systematic institutional coordination to build an integrated data protection ecosystem (Firdaus, 2024; Nirwana *et al.*, 2024).

In addition to harmonizing national regulations, the development of the digital economy also demands alignment between the Personal Data Protection Act (PDP Act) and the international legal regime, particularly regarding cross-border transfers of personal data. The increasing use of cloud computing services, digital transactions, and cross-jurisdictional data exchanges creates a need for international legal cooperation mechanisms capable of effectively protecting personal data. In this context, the implementation of Mutual Legal Assistance (MLA) and regulations governing cross-border data transfers serve as crucial instruments to ensure that data processing remains within the framework of adequate legal protection (Syahputra & Hidayati, 2024). On the other hand, the effectiveness of such harmonization heavily depends on the existence of an independent supervisory authority with the power to conduct oversight, inspections, dispute resolution, and enforce compliance with the provisions of the Personal Data Protection Act (PDP Act). The absence of a fully independent supervisory body can reduce the effectiveness of oversight and create uncertainty about the fulfillment of obligations by data controllers and processors, particularly in cross-sector and cross-border data processing (Ayiliani & Farida, 2024). Therefore, regulatory harmonization, institutional strengthening, and law enforcement coordination are key prerequisites for ensuring that the legal framework of the PDP Act is implemented consistently and provides effective protection for the rights of data subjects within Indonesia's digital ecosystem.

2.4 A Comparative Perspective on Personal Data Protection: Indonesia and the GDPR

Law No. 27 of 2022 on Personal Data Protection (PDP Law) was drafted by adopting several fundamental principles developed in the European Union's General Data Protection Regulation (GDPR), one of the most comprehensive standards for personal data protection in the world. Both legal frameworks treat personal data protection as a fundamental right by recognizing data subjects' rights, the obligations of data controllers and processors, the principle of lawful data processing, transparency, accountability, purpose limitation, and the implementation of adequate security measures in all data processing activities. Furthermore, both the PDP Law and the GDPR grant data subjects the right to obtain information, access, rectify, erase, and restrict the processing of their personal data, along with mechanisms for imposing administrative and criminal sanctions for certain violations (Ramadhani, 2022). These similarities indicate that Indonesian lawmakers are striving to harmonize the national data protection system with international best practices to enhance legal certainty, public trust, and the competitiveness of the digital economy. However, this harmonization does not mean that the legal framework of the PDP Act is entirely identical to the GDPR, as differences still exist in the scope of regulation, institutional mechanisms, and enforcement instruments.

The most notable differences lie in institutional aspects, regulatory scope, and oversight mechanisms. The GDPR explicitly mandates the existence of an independent supervisory authority, data protection impact assessments (DPIAs), automated decision-making, profiling, a one-stop-shop

mechanism, as well as detailed provisions regarding cross-border transfers of personal data based on the principles of adequacy decisions and appropriate safeguards. In contrast, the PDP Act still provides more general regulations regarding these aspects, thus requiring further implementing regulations and harmonization to keep pace with the dynamic developments in digital technology (Taufiq & Kenyo, 2025). Furthermore, the GDPR applies the principle of extraterritorial application, which allows the regulation to apply to data controllers outside the European Union as long as they process data of EU citizens. In contrast, the scope of application of the PDP Law remains relatively limited. Consequently, various studies recommend that Indonesia strengthen its supervisory institutions, clarify risk-based data processing mechanisms, and develop regulations regarding artificial intelligence, profiling, and cross-border data transfers to align with international best practices without disregarding the characteristics of the national legal system (Maleno & Kusumawati, 2024; Simbolon & Juwono, 2022). This comparative approach demonstrates that the GDPR can serve as a normative reference for improving the implementation of the Personal Data Protection Act (PDP Act), particularly regarding legal certainty, the effectiveness of oversight, and the protection of data subjects' rights in the era of digital transformation.

3. Research Method

This study is a normative legal research project that aims to analyze the legal framework for personal data protection within the Indonesian legal system following the enactment of Law No. 27 of 2022 on Personal Data Protection (PDP Law). This study focuses on legal norms (law in books) to examine the legal protection of data subjects' rights, the obligations of data controllers and processors, the relationship between the PDP Act and sectoral regulations, and the legal protection mechanisms for personal data. Therefore, this study does not measure implementation effectiveness through empirical data but rather evaluates the implementation of legal norms based on primary legal sources and official documents related to the application of the PDP Act. A normative legal study was chosen because it is suitable for interpreting statutory provisions, identifying legal ambiguity, analyzing regulatory harmonization, and formulating legal arguments regarding personal data protection issues (Muzairoh *et al.*, 2024).

This study employs three approaches: the statute approach, the conceptual approach, and the comparative approach. The comparative approach is used to examine provisions in the 1945 Constitution of the Republic of Indonesia, Law No. 27 of 2022 on Personal Data Protection, Law No. 11 of 2008 on Electronic Information and Transactions, as last amended by Law No. 1 of 2024, Government Regulation No. 71 of 2019 on the Implementation of Electronic Systems and Transactions, as well as other sectoral regulations related to the processing of personal data. A conceptual approach (conceptual approach) is used to analyze the concepts of the right to privacy, constitutional rights, personal data protection, legal liability, and data protection principles based on legal doctrine and scholarly literature. Furthermore, a comparative approach is used to compare the legal framework of the Personal Data Protection Act with the General Data Protection Regulation (GDPR), particularly regarding the lawful basis for data processing, the rights of data subjects, the obligations of data controllers, cross-border data transfers, oversight mechanisms, and law enforcement.

The legal materials used consist of primary, secondary, and tertiary sources directly related to the research subject. Primary legal materials include the 1945 Constitution of the Republic of Indonesia, Law No. 27 of 2022 on Personal Data Protection, Law No. 11 of 2008 as last amended by Law -Law No.

1 of 2024 on Electronic Information and Transactions, Government Regulation No. 71 of 2019 on the Implementation of Electronic Systems and Transactions, the General Data Protection Regulation (Regulation (EU) 2016/679), as well as official government documents related to personal data protection. Secondary legal sources consist of scientific journal articles, books, research findings, and legal doctrines addressing personal data protection. In contrast, tertiary legal sources include legal dictionaries, legal encyclopedias, and other scholarly references used to clarify legal concepts.

Legal materials were collected through library research by identifying, cataloging, classifying, and evaluating all legal materials relevant to the research issue. The analysis was conducted qualitatively using a descriptive-analytical method through systematic interpretation of statutory provisions, horizontal harmonization among regulations, conceptual analysis of legal doctrines, and a comparative analysis between the Personal Data Protection Act (PDP Act) and the General Data Protection Regulation (GDPR). Furthermore, the discussion of personal data breach cases in this study is used solely as normative illustrations based on official documents, regulatory reports, or published rulings; thus, it is not intended as an empirical analysis of compliance levels or the effectiveness of the PDP Act's implementation. This approach is expected to yield a comprehensive doctrinal analysis of the legal framework for personal data protection, regulatory harmonization, and the development of a personal data protection system in Indonesia.

4. Results and Discussion

4.1 Analysis Results

4.1.1 *Legal Protection of Personal Data in Indonesia Following the Enactment of Law No. 27 of 2022 on the Protection of Personal Data*

Advances in digital technology have transformed the way people interact, conduct transactions, and utilize various public and private services. In this digital transformation, personal data no longer serves merely as a means of identifying individuals, but has also become a strategic asset with economic, social, and legal value. The collection, storage, use, disclosure, transfer, and processing of personal data through various digital platforms increase the risk of privacy rights violations if not accompanied by adequate legal protection mechanisms. Therefore, the protection of personal data is no longer viewed merely as an information security issue, but rather as a legal framework aimed at ensuring legal certainty, the protection of constitutional rights, and the accountability of every party that processes personal data.

Theoretically, the protection of personal data is part of the right to privacy, which is recognized as a human right. The right to privacy grants every individual the authority to determine how their personal data is collected, used, accessed, corrected, or disclosed to third parties. In the context of Indonesian law, this right derives its constitutional legitimacy from Article 28G(1) of the 1945 Constitution of the Republic of Indonesia, which guarantees protection of the person, honor, dignity, and sense of security of every citizen. This constitutional recognition is further operationalized through Law No. 27 of 2022 on Personal Data Protection, which establishes the protection of personal data as a legal right that must be respected in all data processing activities. Thus, the legal basis for protection under the Personal Data Protection Act (PDP Act) is not only oriented toward the administrative interests of electronic system operators but also constitutes the implementation of the state's obligation to protect citizens' constitutional rights in the digital space.

Following the enactment of Law No. 27 of 2022, the legal framework for personal data protection underwent a fundamental shift, as its provisions are no longer scattered across various sectoral regulations but are now consolidated within a single legal regime characterized as *lex specialis*. Prior to the enactment of the Personal Data Protection Act (PDP Act), provisions regarding personal data were scattered across the Electronic Information and Transactions Act and its implementing regulations; consequently, the scope of data subjects' rights, the obligations of data controllers, and dispute resolution mechanisms had not been comprehensively regulated. The PDP Act provides legal certainty through more systematic regulations concerning the definition of personal data, data processing principles, the rights of data subjects, the obligations of data controllers and processors, the transfer of personal data, and mechanisms for legal liability for personal data breaches. Therefore, the changes brought about by the Personal Data Protection Act are not merely normative but also reconstruct the legal relationship between data subjects, data controllers, and the state in the operation of electronic systems.

4.1.2 *Legal Protection of Personal Data in Indonesia Following the Enactment of Law No. 27 of 2022 on the Protection of Personal Data*

One of the fundamental changes introduced by the PDP Act is a stronger recognition of data subjects' rights as the core of legal protection for personal data. Unlike previous regulations, which did not provide a comprehensive formulation of these rights, the PDP Law explicitly grants data subjects the right to obtain information regarding the identity of the data controller, the legal basis for processing, the purposes of processing, as well as the right to access, supplement, update, correct, terminate processing, delete, and destroy personal data in accordance with the provisions of the law. These rights reflect the application of the principle of informational self-determination—that is, the right of every individual to determine how others process their personal data. Thus, legal protection under the PDP Act is not only repressive through the imposition of sanctions but also preventive by granting legal control to data subjects throughout the entire personal data processing cycle.

In addition to regulating the rights of data subjects, the Personal Data Protection Act also establishes obligations that data controllers and processors must fulfill. Data controllers are required to ensure that all data processing is conducted transparently, ethically, and in a purpose-oriented manner, and that the most effective security measures are employed. These obligations constitute the implementation of the principles of lawfulness, fairness, transparency, and accountability, which require every data controller to ensure that processing is carried out on a valid legal basis, in accordance with predetermined purposes, and accompanied by the implementation of technical and organizational measures to protect the confidentiality, integrity, and availability of personal data. From an administrative law perspective, data controllers are not only responsible for administrative compliance but also bear legal liability in the event of a violation of the obligations outlined in the Personal Data Protection Act (PDP Act). Therefore, the formulation of these norms underscores that the protection of personal data is a shared responsibility among the state, data controllers, and data processors in the operation of electronic systems. These requirements promote the application of the principles of accountability and responsibility, which form the cornerstone of modern data protection. Thus, the responsibility for data protection rests not only with the state but also with every individual who collects and processes data on behalf of the public (Santoso & Dinata, 2025).

4.2 Discussion

4.2.1 Challenges and Prospects for the Implementation of Personal Data Protection in Indonesia Following the Enactment of Law No. 27 of 2022 on Personal Data Protection

The enactment of Law No. 27 of 2022 on Personal Data Protection (PDP Law) marks a significant step in the reform of Indonesia's legal system regarding personal data protection. This law provides a more comprehensive legal framework compared to previous regulations, which were scattered across various sectoral regulations. Through provisions regarding the rights of data subjects, the obligations of data controllers and processors, the principles of personal data processing, data transfer mechanisms, as well as administrative and criminal sanctions, the PDP Act seeks to establish a data protection regime that is in line with the development of the digital economy and the need to protect the constitutional rights of citizens. Therefore, the PDP Act is intended not only to provide legal certainty for data subjects but also to establish data governance standards that must be adhered to by all entities processing personal data.

Nevertheless, from a normative legal perspective, the success of the PDP Act's implementation is determined not only by the comprehensiveness of the law's provisions but also by the consistency of its harmonization with sectoral regulations, the clarity of the division of authority among agencies, and the availability of effective oversight and enforcement mechanisms. In a state governed by the rule of law, the existence of legal norms does not automatically guarantee the effectiveness of legal protection if those norms are not supported by institutional frameworks, implementing regulations, and interpretive mechanisms that provide legal certainty for stakeholders. Thus, the analysis of the implementation of the Personal Data Protection Act (PDP Act) in this study is not aimed at empirically measuring the level of compliance by the public or organizations, but rather at evaluating whether the legal framework established has been able to provide adequate legal protection against the processing of personal data within the Indonesian legal system.

From a doctrinal perspective, several provisions in the PDP Act still require further regulation to be effectively applied. For example, regulations concerning the relationship between data controllers and data processors, the transfer of personal data outside Indonesia, the division of supervisory authority, and dispute resolution mechanisms still need to be synchronized with sectoral regulations and implementing regulations. These conditions indicate that the challenges in implementing the PDP Act are not solely due to low compliance among data processors but are also influenced by the need to harmonize legal norms to prevent multiple interpretations in their application. Therefore, discussions regarding the implementation of the PDP Act should be understood as an evaluation of the effectiveness of its legal framework, rather than as an empirical assessment of public or organizational behavior.

4.2.2 Challenges and Prospects for the Implementation of Personal Data Protection in Indonesia Following the Enactment of Law No. 27 of 2022 on Personal Data Protection

One key indicator in evaluating the implementation of the Personal Data Protection Act (PDP Act) is the emergence of various personal data breach cases involving electronic system operators, both in the public and private sectors. From the perspective of normative legal research, these cases are not used to measure an organization's level of compliance empirically, but rather as illustrations of how the legal norms established in the PDP Act are confronted with concrete challenges in practice. The existence of

data breach cases indicates that legal protection for personal data depends not only on the existence of legal norms but also on the effectiveness of implementing data controllers' obligations, oversight mechanisms, and law enforcement regarding violations in the processing of personal data.

One of the main challenges is the high number of personal data breaches that have occurred in recent years. Several data breach cases affecting both government agencies and the private sector indicate that the information security systems implemented by many data controllers remain inadequate. The BPJS Kesehatan data breach, the telecommunications company customer data breach, and the voter data breach related to the General Election Commission demonstrate that personal data management still faces significant risks. These cases highlight the importance of fulfilling data controllers' obligations under the Personal Data Protection Act (PDP Act), particularly the obligation to maintain the confidentiality, integrity, and availability of personal data through the implementation of adequate technical and organizational measures. Thus, data breaches are not only viewed as failures of information technology systems but also have the potential to result in legal consequences if a violation of the obligations outlined in the Personal Data Protection Act is proven. This phenomenon demonstrates that regulations will not be effective unless they are implemented through adequate information security standards and sound data protection governance within every organization that processes personal data (Saly *et al.*, 2023).

From a doctrinal perspective, these various data breach incidents also highlight the importance of the relationship between the Personal Data Protection Act and sector-specific regulations regarding electronic system security. The obligations of data controllers are not limited to obtaining the consent of data subjects but also include the obligation to secure data, prevent unauthorized access, document security incidents, and take remedial measures in the event of a personal data protection breach. Therefore, the occurrence of data breaches should be understood as a basis for evaluating the adequacy of legal norms, the effectiveness of coordination among authorities, and the need to improve oversight mechanisms—not merely as an indicator of weak compliance by the public or organizations.

In addition to institutional challenges and electronic system security, advancements in Artificial Intelligence (AI) technology introduce a new dimension to personal data protection. The use of AI enables data controllers to perform automated processing of personal data on a large scale for various purposes, such as analyzing user behavior, profiling, personalizing services, and algorithm-based decision-making. From a legal perspective, these practices increase the risk of privacy rights violations if carried out without a valid legal basis, without transparency regarding the purpose of processing, or without providing data subjects the opportunity to know and control the use of their personal data. Therefore, AI-based data processing must remain subject to the principles of legality, purpose limitation, proportionality, accountability, and the protection of data subjects' rights as stipulated in the Personal Data Protection Act (PDP Act).

Advances in artificial intelligence (AI) technology also present new challenges in the processing of personal data. The use of AI enables the automated collection and analysis of large amounts of data. On the one hand, this technology helps improve the efficiency of public services and business operations. However, the use of AI has the potential to lead to profiling, automated decision-making, and large-scale data processing that can affect the rights and freedoms of data subjects if not accompanied by adequate transparency and oversight mechanisms. These conditions indicate that personal data protection can no longer focus solely on information system security but must also address algorithmic accountability, clarity of processing purposes, and the management of risks posed by digital technology. Therefore, the implementation of the Personal Data Protection Act (PDP Act) must

accommodate increasingly complex technological developments to ensure the integrity and protection of personal data. In this context, applying a risk-based approach is essential for identifying the level of risk associated with data processing, determining proportionate mitigation measures, and ensuring that the use of AI remains within the framework of protecting citizens' constitutional rights. The risk-based approach, which is applied in various international data protection regimes, can serve as one option for strengthening the protection of personal data in Indonesia.

From a doctrinal perspective, strengthening oversight of AI-based data processing requires not only data controllers' compliance with legal obligations but also implementing regulations that establish standards for algorithmic transparency, documentation of processing procedures, audit mechanisms, and procedures for addressing violations arising from the use of automated systems. Thus, the challenge of implementing the Personal Data Protection Act (PDP Act) in the era of artificial intelligence is not merely related to technological developments but also concerns the legal system's ability to anticipate new risks arising from algorithm-based personal data processing in an accountable and responsible manner.

From a comparative law perspective, Law No. 27 of 2022 on Personal Data Protection (PDP Act) adopts several fundamental principles developed in the General Data Protection Regulation (GDPR), such as the principle of legality of data processing, consent, transparency, accountability, purpose limitation, and recognition of data subjects' rights. Nevertheless, the scope of regulation under these two legal regimes still exhibits several fundamental differences. The GDPR provides more detailed regulations regarding the legal basis for data processing, the application of Data Protection Impact Assessments (DPIAs), automated decision-making, profiling, breach notification mechanisms, and cross-border data transfers based on the principles of adequacy decisions and appropriate safeguards. Conversely, the PDP Act still provides more general provisions regarding these aspects, thus requiring further implementing regulations and interpretation to provide legal certainty in the face of increasingly complex developments in digital technology. This situation indicates that harmonization with international standards cannot be achieved solely through the adoption of general principles but also requires the strengthening of operational norms and supervisory institutions to ensure the effective implementation of personal data protection.

In addition to differences in the substance of the regulations, the two legal regimes also differ in institutional and enforcement aspects. The GDPR is supported by an independent supervisory authority that can conduct oversight and investigations, impose administrative sanctions, and resolve data subject complaints independently. In contrast, the implementation of the Personal Data Protection Act (PDP Act) still faces challenges in strengthening the supervisory authority and aligning its powers with those of various sectoral regulators. Therefore, the prospects for developing a personal data protection system in Indonesia depend not only on refining the substance of the PDP Act but also on establishing an independent supervisory body, harmonizing with sectoral regulations, drafting implementing regulations on risk-based data processing, and strengthening oversight mechanisms for cross-border data processing and artificial intelligence-based technologies. Thus, a comparative perspective with the GDPR indicates that improvements to Indonesia's personal data protection system must be directed toward strengthening legal certainty, the effectiveness of law enforcement, and the more comprehensive protection of data subjects' rights.

5. Concluding Remarks and Recommendation

This study aims to analyze the legal framework for personal data protection in Indonesia following the enactment of Law No. 27 of 2022 on Personal Data Protection (PDP Law) and to identify the challenges in its implementation through a normative legal research approach incorporating statutory, conceptual, and comparative perspectives. Based on the results of the analysis, this study found that the PDP Act has established a more comprehensive legal regime for personal data protection compared to previous regulations through the recognition of data subjects' rights, the regulation of the obligations of data controllers and processors, the principles of personal data processing, as well as mechanisms for administrative and criminal liability. However, the main findings of this study indicate that the challenges in implementing the PDP Act are not solely due to low compliance among data processors, but also stem from the ongoing need for harmonization between the PDP Act and sectoral regulations, the suboptimal institutional framework of the independent supervisory authority, and the need to refine norms regarding data processing based on digital technology, including automated processing, profiling, and cross-border transfers of personal data.

This study makes a theoretical contribution by expanding the legal analysis of personal data protection through a doctrinal analysis that positions the Personal Data Protection Act as part of the national legal system that must be harmonized with sectoral regulations and systematically compared with the General Data Protection Regulation (GDPR). From a practical and policy perspective, the results of this study highlight the importance of drafting more comprehensive implementing regulations, strengthening independent data protection supervisory institutions, improving coordination among authorities, and developing risk-based oversight mechanisms for data processing (risk-based approach). Thus, the novelty of this study lies in its analysis of the interrelationships among regulations, the construction of institutional authority, and the legal implications of digital technology developments for the implementation of the Personal Data Protection Act—aspects that have not been systematically examined in previous research.

This study has limitations because it employs a normative legal approach focused on the analysis of legislation, legal doctrine, and secondary legal sources; consequently, it does not evaluate the implementation of the Personal Data Protection Act based on empirical data regarding the level of compliance by data controllers or the effectiveness of law enforcement in the field. Furthermore, this study has not thoroughly examined the development of implementing regulations for the PDP Act or law enforcement practices following the establishment of technical policies in the field of personal data protection. Therefore, future research is recommended to combine normative and empirical approaches to evaluate the effectiveness of the PDP Act's implementation, analyze the application of the principles of accountability and privacy by design across various strategic sectors, and examine regulatory developments related to artificial intelligence, profiling, cross-border data transfer, and the governance of personal data protection within Indonesia's digital ecosystem.

Statement of Use of Generative AI

During the preparation of this work, the author used generative artificial intelligence tools to support the scientific writing process. Grammarly was used to check grammar, refine writing style, and improve clarity in scientific writing. All interpretations, analyses, and conclusions presented in this study are the sole responsibility of the author.



References

- Abita, C., Irwandi, & Amin, M. (2024). Perbandingan Perlindungan Data Pribadi Antara Undang-Undang Nomor 27 Tahun 2022 Dan Undang-Undang Nomor 1 Tahun 2024 . *Limbago: Journal of Constitutional Law*, 4(2), 205–214. <https://doi.org/10.22437/limbago.v4i2.34161>
- Aqilah, R., Waryenti, D., & Susanti, P. (2022). Tanggung Jawab Negara Mengenai Perlindungan Data Pribadi Berdasarkan Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi. *Jurnal Ilmiah Kutei*, 23, 158–172.
- Ayiliani, F. M., & Farida, E. (2024). Urgensi Pembentukan Lembaga Pengawas Data Pribadi sebagai Upaya Perlindungan Hukum terhadap Transfer Data Pribadi Lintas Negara. *Jurnal Pembangunan Hukum Indonesia*, 6(3), 431–455. <https://doi.org/10.14710/jphi.v6i3.431-455>
- Budiarta, I. N. P., Dharsana, I. M. P., & Kresnadjaja, I. (2023). Penguatan Konstruksi Hukum Perihal Perlindungan Data Pribadi. *Jurnal Magister Hukum Udayana (Udayana Master Law Journal)*; Vol 12 No 1 (2023)DO - 10.24843/JMHU.2023.V12.I01.P05. <https://doi.org/10.24843/JMHU.2023.v12.i01.p05>
- Fauzy, E., & Nabila Alif Radika Shandy. (2023). Hak Atas Privasi dan Politik Hukum Undang-Undang Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi. *Lex Renaissance*, 7(3), 445–461. <https://doi.org/10.20885/JLR.vol7.iss3.art1>
- Firdaus, F. H. (2024). Perlindungan Dan Kepastian Hukum Bagi Pengendali Data Pribadi Di Masa Depan. *Masalah-Masalah Hukum*, 53(2), 135–144. <https://doi.org/10.14710/mmh.53.2.2024.135-144>
- 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(1), 20–29. <https://doi.org/10.58812/eslhr.v3i01.351>
- K, N. A., & Makkawaru, Z. (2024). Legal Protection of Personal Data from the Perspective of Human Rights in Indonesia. *Indonesian Journal of Legality of Law*, 7(1), 46–51. <https://doi.org/10.35965/ijlf.v7i1.5267>
- Kurdi, K., & Cahyono, J. (2024). Perlindungan Data Pribadi di Era Digital Berdasarkan Undang-Undang Nomor 27 Tahun 2022. *JUNCTO: Jurnal Ilmiah Hukum*, 6(2), 330–339. <https://doi.org/10.31289/juncto.v6i2.5443>
- Maleno, M., & Kusumawati, A. (2024). Comparative Analysis of Indonesia's Personal Data Protection Law with the European Union and California Regulations to Identify Best Practices in Protecting Public Privacy Rights. *Indonesia Law College Association Law Journal*, 3(2), 91–98. <https://ejournal.psthi.or.id/index.php/ILCALaw/article/view/21>
- Manurung, E. A. P., & Thalib, E. F. (2023). Tinjauan Yuridis Perlindungan Data Pribadi Berdasarkan Uu Nomor 27 Tahun 2022. *Jurnal Hukum Saraswati (JHS)*, 4(2), 139–148. <https://ejournal.unmas.ac.id/index.php/JHS/article/view/5941>
- Nirwana, D., Nurjannah, E., Marpaung, C. R. A., & Wijaya, H. A. (2024). Analisis Kebijakan Keamanan Cyber: Study Kasus Implementasi Perlindungan Data Pribadi Dalam Era Digital. *JlIP - Jurnal Ilmiah Ilmu Pendidikan*, 7(7 SE-), 7364–7373. <https://doi.org/10.54371/jiip.v7i7.4790>
- Nirwana, M. A. (2022). Perlindungan Hukum Terhadap Data Pribadi Sebagai Hak Privasi Individual. *AL WASATH Jurnal Ilmu Hukum*, 3(2), 93–104. <https://doi.org/10.47776/alwasath.v3i2.609>
- Palit, S. M. L., & Purba, T. L. D. (2025). Legal Perspective on Data Privacy Protection as a Human Right in Indonesia. *The Easta Journal Law and Human Rights*, 4(1), 24–32. <https://doi.org/10.58812/eslhr.v4i01.783>
- Putri, N. M. D. G., Mahendrawati, N. L. M., & Ujianti, N. M. P. (2024). Perlindungan Hukum Terhadap Data Pribadi Warga Negara Indonesia Berdasarkan Undang-Undang Nomor 27 Tahun 2022. *Jurnal Preferensi Hukum*, 5(2 SE-Articles), 240–245. <https://www.ejournal.warmadewa.ac.id/index.php/juprehum/article/view/8087>
- Ramadhani, S. A. (2022). Komparasi Perlindungan Data Pribadi di Indonesia dan Uni Eropa. *Jurnal Hukum Lex Generalis*, 3(1), 73–84. <https://doi.org/10.56370/jhlg.v3i1.173>
- Ravinka, N. A., & Widiatedja, I. (2022). What should Indonesia learn from rights to data privacy under the GDPR.



- Kertha Semaya *J Ilmu Huk*, 10(3). <https://doi.org/10.24843/KS.2022.v10.i03.p09>
- Rinjani, M. A., & Firmansyah, R. (2025). Hambatan Implementasi UU 27/2022 dan Strategi Penguatan Perlindungan Data Pribadi di Indonesia. *Jurnal Analisis Hukum*, 8(1), 70–83. <https://doi.org/10.38043/jah.v8i1.6793>
- Rizki Bachtiar, F., Ardytia, W., & Brian Wicaksono, D. (2025). Analisis Penegakan Hukum Data Pribadi Pada Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi Di Indonesia. *AMAR*, 3(2), 101–110. <https://doi.org/10.62734/amar.v3i2.762>
- Saly, J. N., Artamevia, H., Kheista, K., Gulo, B. J. S., Rhemrev, E. A., & Christie, M. (2023). Analisis perlindungan data pribadi terkait UU No. 27 Tahun 2022. *Jurnal Serina Sosial Humaniora*, 1(3), 145–153. <https://journal.untar.ac.id/index.php/JSSH/article/view/28615>
- Santoso, M. A., & Dinata, U. (2025). Perlindungan Hukum Bagi Konsumen Dan Tanggung Jawab Pidana Pelaku Penyalahgunaan Data Pribadi. *ANDREW Law Journal*, 4(1), 1–6. <https://doi.org/10.61876/alj.v4i1.39>
- 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. <https://doi.org/10.31314/pjia.11.2.178-190.2022>
- Syahputra, R. A., & Hidayati, M. N. (2024). Implementasi Mutual Legal Assistance (MLA) untuk Perlindungan Data Pribadi Pengguna Layanan Komputasi Awan di ASEAN. *Sang Pencerah: Jurnal Ilmiah Universitas Muhammadiyah Buton*, 10(3), 825–838. <https://doi.org/10.35326/pencerah.v10i3.5883>
- Taufiq, M., & Kenyo, A. S. (2025). The Legal Protection of Personal Data in the Digital Era: A Comparative Study of Indonesian Law and the GDPR. *International Journal of Business, Law, and Education*, 6(2), 1260–1268. <https://doi.org/10.56442/ijble.v6i2.1178>
- Widodo, J. E., Suganda, A., & Tubagus Achmad Darodjat. (2024). Data Privacy And Constitutional Rights In Indonesia: Data Privacy And Constitutional Rights In Indonesia. *Pena Law: International Journal of Law*, 2(2). <https://doi.org/10.56107/penalaw.v2i2.187>

Corresponding author

Michelle Nabila Andaista Bangsu can be contacted at: bangsumichelle@gmail.com

