Lex Publica
Jurnal Ilmu Hukum Asosiasi Pimpinan Perguruan Tinggi Hukum Indonesia
e-ISSN: 2579-8855
p-ISSN: 2354-9181
https://journal.appthi.org/index.php/lexpublica

Criminal Sanctions and Personal Data Protection in Indonesia

Kukuh Dwi Kurniawan[1*], Deassy J.A. Hehanussa[2], Rahmat Setiawan[3], Indah Susilowati[4], Sopian[5], Desmarani Helfisar[5]

[1] Faculty of Law, Universitas Muhammadiyah Malang, Malang, Indonesia
[2] Faculty of Law, Universitas Pattimura, Ambon, Indonesia
[3] Faculty of Law, Universitas Muhammadiyah Luwuk, Banggai, Indonesia
[4]Faculty of Health Technology and Management, Institut Ilmu Kesehatan Bhakti Wiyata Kediri, Kediri, Indonesia
[5] Faculty of Sharia, Universitas Islam Batang Hari, Batang Hari, Indonesia

**Corresponding author: kukuhdwik@umm.ac.id*

Abstract. This research analyzes Indonesia's Law Number 27 of 2022 on Personal Data Protection (Law on Personal Data Protection), focusing on its regulatory framework and institutional strengthening efforts. The study employs a normative legal research approach with a descriptive-analytical method, examining primary legal materials such as Law Number 27 of 2022 and secondary sources including relevant academic literature. To provide a global perspective, comparisons are drawn with the General Data Protection Regulation (GDPR) in the European Union, the Personal Data Protection Act (PDPA) in Singapore, and the Act on the Protection of Personal Information (APPI) in Japan. The findings reveal that while the Law on Personal Data Protection provides a comprehensive framework for personal data protection, its implementation faces significant challenges, including low public awareness, insufficient readiness in the business sector, and limited enforcement capacity of supervisory institutions. Strengthening institutional frameworks and enhancing public understanding of data privacy rights are critical steps toward addressing these challenges. Although criminal sanctions are stipulated in the law, their application has yet to be evaluated in depth, as this research primarily focuses on regulatory analysis. Suggestions include developing robust technological and organizational measures to secure data and fostering international collaboration in managing cross-border data flows to align with global standards. Further research is recommended to assess the effectiveness of criminal sanctions in deterring data breaches and their role in enhancing the overall efficacy of Indonesia's personal data protection framework.

Keywords: Personal Data Protection, Law Number 27 of 2022, Institutional Strengthening, Data Privacy, General Data Protection Regulation

Abstrak. *Penelitian ini bertujuan untuk menganalisis secara mendalam mekanisme perlindungan data pribadi dalam Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi di Indonesia, serta menilai efektivitas sanksi pidana yang diterapkan untuk pelanggaran terkait perlindungan data. Penelitian ini menggunakan metode hukum normatif dengan pendekatan deskriptif-analitis, yang menitikberatkan pada analisis dokumen hukum primer, seperti Undang-Undang No. 27 Tahun 2022, serta dokumen hukum sekunder, termasuk artikel akademik dan jurnal yang relevan. Penelitian juga melakukan perbandingan dengan regulasi internasional seperti General Data Protection Regulation (GDPR) di Uni Eropa, Personal Data Protection Act (PDPA) di Singapura, dan Act on the Protection of Personal Information (APPI) di Jepang untuk mendapatkan perspektif global. Hasil penelitian ini menunjukkan bahwa meskipun Undang-Undang No. 27 Tahun 2022 telah mengatur perlindungan data secara komprehensif, terdapat tantangan besar dalam implementasinya, terutama terkait dengan kesadaran publik, kesiapan sektor bisnis, serta kapasitas lembaga pengawas untuk menegakkan hukum. Sanksi pidana yang diatur, meskipun signifikan, memerlukan penerapan yang konsisten dan tegas untuk menciptakan efek jera yang optimal. Selain itu, penelitian ini juga menemukan bahwa peran teknologi dalam meningkatkan keamanan data, serta kerjasama internasional dalam menangani transfer data lintas batas, sangat penting untuk memastikan bahwa data pribadi warga negara Indonesia terlindungi sesuai standar global. Kesimpulannya, untuk meningkatkan efektivitas Undang-Undang No. 27 Tahun 2022, perlu dilakukan penguatan kelembagaan, sosialisasi yang lebih luas tentang hak-hak individu terkait data pribadi, serta pengembangan teknologi dan regulasi yang memungkinkan penerapan perlindungan data yang lebih baik.*

Kata kunci: *Perlindungan Data Pribadi, Undang-Undang Nomor 27 Tahun 2022, Penguatan Kelembagaan, Privasi Data, Peraturan Umum Perlindungan Data*

1. Introduction

Personal data protection has become an important concern at the global level, alongside personal data privacy, which has become a worldwide issue as information technology advances. In the digital age, personal data can often be misused; thus, several nations have passed laws protecting individual privacy rights.[1] The first data protection legislation was passed in 1970 in Hesse, Germany, to safeguard personal data from third parties. The 2016 European Union approval of the General Data Protection Regulation (GDPR) expanded personal data protection in Europe. International emphasis has been placed on personal data protection.[2] Since 1980, international organizations like the OECD have produced privacy recommendations.[3] In an age of global cross-border commerce and multinational corporations collecting and processing user data, these rules seek to prevent personal data abuse. They stress transparency, consent, and fairness in data processing. Due to the (GDPR), several nations outside the EU are adopting personal data protection legislation to comply with global norms and facilitate cross-border commercial and trade cooperation that depends on data flows.[4]

Personal data protection begins with the awareness that personal information is a human right. The 1945 Indonesian Constitution protects personal rights, including data. With Law Number 27 of 2022 on Personal Data Protection, Indonesia's special data protection law has now been legalized. This legislation addresses the essential need for legal clarity in the digital age, when personal data is routinely exploited or exchanged without consent.[5] It protects personal data by granting individuals the right to control and safeguard their data, and by requiring entities that administer it to keep it secure and confidential. The Act defines personal data, grants data owner rights, assigns duties to data controllers, and describes data processing methods. Two types of personal data exist: general and particular. Health, biometric, genetic, criminal, children, and other sensitive data

[1] Jufryanto Puluhulawa et al., "The Concept of Cyber Insurance as a Loss Guarantee on Data Protection Hacking in Indonesia," *Law, State and Telecommunications Review* 15, no. 2 (2023): 140.

[2] Paul Voigt, and Axel Von dem Bussche, "*The eu General Data Protection Regulation (GDPR)*," (Cham: Springer International Publishing, 2017): 3245.

[3] Angel Gurria, "OECD Employment Outlook 2020: Worker Security and The Covid-19 Crisis," *OECD Employment Outlook* 14, no. 5 (2020): 191.

[4] Chris Jay Hoofnagle, Bart Van Der Sloot, and Frederik Zuiderveen Borgesius, "The European Union general data protection regulation: what it is and what it means," *Information & Communications Technology Law* 28, no. 1 (2019): 69.

[5] Al Sentot Sudarwanto and Dona Budi Budi Kharisma, "Comparative Study of Personal Data Protection Regulations in Indonesia, Hong Kong and Malaysia," *Journal of Financial Crime* 29, no. 4 (2021): 571.

could have catastrophic ramifications if mishandled. General data includes information such as name, gender, religion, and marital status.

The rights of data subjects' people whose data is collected, processed, or used are crucial to this Act. Under the Act, data subjects have the right to know who collects their data, why it is collected, and how it is used. Data subjects may access, amend, update, or delete their data if it is no longer required.[6] These rights strengthen digital privacy protection. Law No. 27 of 2022 also compels data controllers to safeguard personal data, in addition to protecting data subjects' rights. Data controllers must take both technological and organizational steps to protect data against unauthorized access, disclosure, and modification. To prevent data leakage, data controllers must use data encryption, access restrictions, and conduct frequent audits.[7]

Additionally, this law imposes severe penalties on parties that breach personal data protection laws. Personal data protection breaches are criminalized under Chapter 14 of Law Number 27 of 2022. Anyone who willfully and without permission obtains or collects personal data for their own gain may be imprisoned for up to five years or fined five billion rupiah. Anyone who willfully exposes or uses personal data without authorization faces the same punishment. Creating or falsifying personal data may result in a six-year prison sentence or a fine of six billion rupiah. These harsh punishments demonstrate Indonesia's commitment to data protection. Corporate data protection violators may face jail terms, penalties, company freezes, premises closures, and license revocations. The government may also cooperate internationally to resolve foreign personal data infractions under this statute.[8] Given the global data flow and the possibility of foreign company violations, this is crucial.

This research has high urgency in the context of personal data protection in Indonesia, especially after the ratification of Law Number 27 of 2022 concerning Personal Data Protection (UU PDP). In previous studies highlighted that although the PDP Law has similarities with the GDPR in the European Union, technical implementations such as the management of administrative and criminal sanctions have not been fully structured clearly.[9] In addition previous research underlined

[6] Evelyn Angelita Pinondang Manurung, "The Right to Privacy Based on the Law of the Republic of Indonesia Number 27 of 2022," *Journal of Digital Law and Policy* 2, no. 3 (2023): 56.

[7] Tabitha Fransisca Romauli Nababan and Shevanna Putri Cantiqa, "Mengoptimalkan Implementasi UU No. 27 Tahun 2022 Dengan Penetration Test Dan Vulnerability Assessment Pada Kasus Pembobolan Data Aplikasi Dana," *Jurnal Hukum, Politik Dan Ilmu Sosial* 3, no. 3 (2024): 94.

[8] Hanita Mayasari, "A Examination on Personal Data Protection in Metaverse Technology in Indonesia: A Human Rights Perspective," *Journal of Law, Environmental and Justice* 1, no. 1 (2023): 75.

[9] Valentina Ancillia Simbolon and Vishnu Juwono, "Comparative Review of Personal Data Protection Policy in Indonesia and The European Union General Data Protection Regulation," *Publik (Jurnal Ilmu Administrasi)* 11, no. 2 (2022): 121.

that the PDP Law still faces major challenges in its implementation in the Internet of Things (IoT) sector, especially regarding data protection based on advanced technology.[10]

This study differs from previous studies by focusing on two main aspects, namely how the PDP Law provides a mechanism for protecting personal data and the effectiveness of the criminal sanctions regulated therein. This study uses a descriptive-analytical approach to fill the research gap in the form of a lack of in-depth evaluation of the criminal sanction mechanism and the extent to which these sanctions can provide a deterrent effect in preventing personal data violations. In addition, the focus on comparisons with international regulations such as GDPR, Singapore's PDPA, and Japan's APPI provides a global context that is rarely highlighted comprehensively in previous studies.

Criminal penalties governed under Law No. 27 of 2022 represent the second issue. The prevention of personal data breaches relies on criminal consequences.[11] Criminal penalties governed under Law No. 27 of 2022 focus on addressing violations related to personal data protection. This legislation aims to deter personal data breaches through severe punitive measures, including imprisonment and substantial fines for both individuals and corporations. For instance, the law stipulates imprisonment of up to five years or fines of up to five billion rupiah for individuals who unlawfully collect or misuse personal data. However, the effectiveness of these penalties in preventing violations remains a critical issue. While the penalties indicate Indonesia's commitment to personal data protection, their practical application and enforcement are constrained by challenges such as limited institutional capacity, lack of public awareness, and the evolving nature of cyber threats.

To align with its objectives, this research evaluates how effectively these punishments are implemented and their role in reducing data protection violations. The study highlights the gaps in the enforcement framework, particularly in ensuring consistent application of penalties and addressing emerging risks, such as the misuse of advanced technologies like artificial intelligence and IoT. Unlike regulations such as the GDPR, which explicitly outline enforcement mechanisms and data protection authorities, Law No. 27 of 2022 lacks robust institutional support to ensure the uniform application of its provisions. The research also investigates legal and technological strategies to strengthen the enforcement of criminal sanctions. Recommendations include establishing a dedicated data

[10] Muhamad Alfat Fauzie, "Securing the Future: Indonesia Personal Data Protection Law and It' S Implication for Internet of Things (IOT) Data Privacy," *Sriwijaya Crimen and Legal Studies* 2, no. 1 (2024): 18.

[11] Arnanda Yusliwidaka, Muhammad Ardhi Razaq Abqa, and Khansadhia Afifah Wardana, "A Discourse of Personal Data Protection: How Indonesia Responsible under Domestic and International Law?," *Pandecta Research Law Journal* 19, no. 2 (2024): 183.

protection authority, improving public and business awareness about personal data rights and responsibilities, and fostering international cooperation in combating cross-border data breaches. By addressing these gaps, the law's criminal sanctions can serve as a more effective deterrent, ensuring that the rights of Indonesian citizens are safeguarded in an increasingly digital world.

2. Research Methods

This study used the normative legal research technique to analyze the normative features of personal data protection and criminal punishments under Law Number 27 of 2022. It addressed the two issue formulations by studying relevant legal documents and literature.[12] This study analyzed primary legal sources, including Law No. 27 of 2022 concerning the Protection of Personal Data and the Electronic Information and Transactions Law, to answer the first problem formulation: how it protects personal data in Indonesia. The research also evaluated secondary legal sources, including books, scientific papers, journals, and academic references on personal data protection in Indonesia and other countries, as well as international standards like the GDPR.

A normative descriptive technique was used to map Law No. 27 of 2022 on personal data protection regulation and comprehend its goals.[13] The research investigated the legislation's provisions on data subjects' rights, data controllers' duties, and law enforcement procedures to safeguard personal data.[14] The juridical-analytical technique was used to address the second issue formulation: what criminal punishments Law No. 27 of 2022 imposes for personal data protection infractions and how effective they are. The legal repercussions of personal data privacy infractions, including imprisonment, fines, and administrative punishments under this law, were examined.[15]

This study used a qualitative descriptive approach as its primary data analysis method. The juridical-analytical technique was specifically utilized to evaluate the effectiveness of criminal punishments under this law. This technique involved

[12] Peter. Mahmud Marzuki, *Penelitian Hukum*, (Jakarta: Kencana Prenada Media Group, 2011), 133.

[13] Arnanda, Abqa, and Wardana, "A Discourse of Personal Data Protection," 197.

[14] Tegar Islami Putra, Akbar Jihadul Islam, and Abdullah Mufti Abdul Rahman, "Integrating Islamic Laws into Indonesian Data Protection Laws: An Analysis of Regulatory Landscape and Ethical Considerations," *Contemporary Issues on Interfaith Law and Society* 3, no. 1 (2024): 102.

[15] Intan Audia Priskarini and Kukuh Tejomurti, "The Role of The Financial Services Authority in The Legal Protection of Privacy Rights in Connection with Personal Data of Fintech Lending Debtor in Indonesia | Peran Otoritas Jasa Keuangan (OJK) dalam Perlindungan Hukum Hak Privasi atas Data Pribadi Konsumen Peminjam Fintech Lending di Indonesia," *Padjadjaran Jurnal Ilmu Hukum* 6, no. 3 (2019): 559.

analyzing the practical application of penalties, their deterrent effect, and the barriers to enforcement. The study also integrated comparative legal analysis to benchmark Indonesia's regulatory framework against international norms, particularly GDPR, PDPA, and APPI.

3. Results and Discussion

3.1. Human Rights and Economic Interests in Personal Data Protection

In the theoretical context of personal data protection, law, IT, and human rights specialists can provide deeper insights. The right to privacy concept, articulated by Warren and Brandeis in their work The Right to Privacy,[16] is frequently applied. They defined privacy as the right to be "left alone" or unbothered in one's private life. This notion has expanded as technology collects and manages personal data, making it part of human rights.[17] They argue that personal data privacy preserves human dignity by giving people complete control over their data. Information rights theory from Alan Westin supports this approach in the present age. Westin argued in *Privacy and Freedom* that privacy is the right to determine how personal information is used and shared.[18] He stated that information technology makes it difficult for people to govern their personal data since it is often acquired and utilized without their permission. Westin emphasized that legislation must actively regulate data access and usage to prevent irresponsible parties from misusing it.[19]

However, in the digital economy, privacy and economic interests are increasingly at odds. Some experts argue that overly strict personal data privacy laws may hamper innovation and economic development, particularly for technology businesses that utilize user data to enhance their services. Richard Posner, as summarized by Singer, argues that data privacy does not necessarily need to be tightly secured.[20] Personal data is a commodity in a capitalist system, and Posner believes customers should recognize that they are "paying" for digital

[16] Tom Goldstein, *Killing the Messenger: 100 Years of Media Criticism,* (New York: Columbia University Press, 2019), 43.

[17] Priskarini and Tejomurti, "The Role of The Financial Services Authority in The Legal," 564.

[18] Stanley I. Benn, "Privacy, Freedom, and Respect for Persons," in *Privacy and Personality* 22, no. 11 (1971): 144.

[19] Alam A. K. M. Mubashwir, Sagar Sharma, and Keke Chen, "SGX-MR: Regulating Dataflows for Protecting Access Patterns of Data-Intensive SGX Applications," *ArXiv e-prints* 7, no. 2 (2020): 2009.

[20] Joseph William Singer, "Legal Realism Now," *California Law Review* 76, no. 3 (1988): 465.

services with their data.[21] This argument promotes monetizing personal data as an economic resource.

This economic strategy has been criticized by human rights experts like for Julie E. Cohen ignoring privacy as a basic human right. Cohen believes privacy encompasses the ability to develop personal identities and live independently without intrusive monitoring, as well as economic ownership over data.[22] In the digital era, civil freedoms depend on personal data security. This topic pits human rights against utilitarian personal data policies. Posner advocates for the utilitarian use of personal data for economic benefit. Many criticize this stance for forsaking individual rights in favor of economic efficiency. Cohen human rights approach emphasizes that personal data is part of an individual's dignity and cannot be treated as a commodity.[23] This position stresses that people have a right to determine how their information is used and opposes the notion that economic gains should trump privacy. This argument highlights the conflict between stricter privacy regulations and the needs of the digital economy. In Europe, the GDPR balances these two goals by imposing strong privacy requirements while enabling data transfers necessary for economic activity.[24]

The debate on personal data protection in Indonesia involves various groups, including academics, lawyers, and policymakers, who are trying to balance human rights and economic needs in the digital era. Bambang Pratama, an academic and researcher at the Department of Business Law at Bina Nusantara University, emphasized the need for reform of personal data protection in Indonesia. He specifically highlighted the importance of adopting the concept of the "right to be forgotten" as an important element in maintaining individual privacy.[25] From the lawyer's perspective, Suhendra Asido Hutabarat, Head of DPC Peradi West Jakarta, emphasized the importance of improving the quality of the legal profession in understanding current issues related to privacy and personal data protection. This aims to ensure that advocates can provide legal services that are in accordance with regulatory and technological developments. Meanwhile, policy makers, such as Commission I of the Indonesian House of Representatives, have been actively involved in discussing the Draft Law on Personal Data Protection (RUU PDP).

[21] Rafael Capurro, Michael Eldred, and Daniel Nagel, *Digital Whoness: Identity, Privacy and Freedom in the Cyberworld,* (Boston: Walter de Gruyter, 2013), 44.

[22] Joy Land, "Cohen-Scali Saguès, Julie," *Encyclopedia of Jews in the Islamic World* 22, no.5 (2010): 166

[23] Julie E. Cohen, "What Privacy Is For," *Harvard Law Review* 126, no. 33 (2013): 1904.

[24] He Li, Lu Yu, and Wu He, "The Impact of GDPR on Global Technology Development," *Journal of Global Information Technology Management* 22, no. 1 (2019): 3.

[25] Tribunnews.com, "Akademisi Sebut Perlindungan Data di RI Butuh Reformasi, Singgung Kebocoran Data e-KTP," Tribunnews.com, 26 December 2024, https://www.tribunnews.com/nasional/2024/12/19/akademisi-sebut-perlindungan-data-di-ri-butuh-reformasi-singgung-kebocoran-data-e-ktp, accessed on December 28, 2024.

The debate among council members covers a variety of issues, including the scope of regulation, personal data rights, and personal data management mechanisms.[26] This discussion shows that there are major challenges in designing laws that can protect individual privacy rights without hindering the growth of the digital economy. Close collaboration between academics, legal practitioners, and policy makers is key to producing effective and adaptive regulations to technological developments.

Law Number 27 of 2022 on Personal Data Protection (Personal Data Protection Law) is a milestone in developing a legal framework that can address digital issues in Indonesia. This legislation expands the protection of data subjects' rights and clarifies the obligations of data controllers and processors. The law regulates data subjects' rights, data controllers' obligations, and data processing procedures to ensure that all personal data management is legal, transparent, and accountable, thereby protecting the privacy rights of Indonesian citizens.[27] Chapter 4, from Articles 5 to 15 of Law No. 27 of 2022, defines the rights of data subjects, which are crucial to personal data protection. Data subjects have the right to know who collects their data, why it is collected, and how it is used. These rights include access to personal data, correction of inaccurate data, and the deletion of data that is no longer needed or relevant. Data subjects also have the right to withdraw their consent for data processing and to object if the decision-making is based exclusively on automated processing, such as profiling with a substantial effect. The legislation grants these rights to empower individuals to maintain their privacy by giving them complete control over their personal data.[28]

The Personal Data Protection Law also imposes strict data protection requirements on data controllers and processors. As stated in Articles 16 to 39, data controllers must acquire personal data in a restricted, targeted, legal, and transparent manner.[29] Each data controller must notify the data subject of processing activities and protect the data from unauthorized use. This legislation also requires data controllers to conduct a Data Protection Impact Assessment (DPIA) whenever data processing poses a high risk to data subjects, particularly

[26] Muhammad Rizieq Firmansyah, "Perlindungan Data Pribadi Dalam Transaksi Elektronik Pra dan Pasca UU Nomor 27 Tahun 2022," Fakultas Syariah dan Hukum UIN Syarif Hidayatullah Jakarta, 2023, https://repository.uinjkt.ac.id/dspace/handle/123456789/76415.

[27] Ferina Widyawati Ayu Silvi and Anom Wahyu Asmorojati, "The Urgency of Establishing a Special Agency of Personal Data Protection and Supervision to Ensure the Indonesian Citizens' Privacy Rights," *Borobudur Law Review* 4, no. 2 (2022): 67.

[28] Endang Lestari and Rasji Rasji, "Legal Study on Personal Data Protection Based on Indonesian Legislation," *Awang Long Law Review* 6, no. 2 (2024): 265.

[29] Dona Budi Kharisma and Alvalerie Diakanza, "Patient Personal Data Protection: Comparing the Health-Care Regulations in Indonesia, Singapore and the European Union," *International Journal of Human Rights in Healthcare* 17, no. 2 (2024): 159.

for automated decision-making that may have legal or significant consequences.[30] The Personal Data Protection Act also prioritizes data security. Data controllers must safeguard personal data against unlawful access, unauthorized disclosure, modification, and destruction under Articles 35–39. To achieve this, data controllers must use encryption, access restrictions, and frequent security assessments. This clause mandates rigorous data security standards, particularly in areas like banking, health, and technology that handle sensitive or large amounts of personal data.[31]

Personal data protection in Indonesia has been a longstanding concern, although emphasis has grown recently. Before Law Number 27 of 2022 on Personal Data Protection, personal data protection legislation was fragmented and incomplete. Law 11 of 2008 on Information and Electronic Transactions (ITE Law) was one of the first to regulate electronic information, including personal data. Law 19 of 2016 revised it.[32] The Electronic Information and Transactions Law requires electronic system organizers to protect personal data by maintaining its confidentiality, integrity, and availability.

The Electronic Information and Transactions Law requires electronic system organizers to protect personal data by maintaining its confidentiality, integrity, and availability.[33] In addition, the Electronic Information and Transactions Law does not define personal data, data owners' rights, or data controllers' duties.[34] Other regulations have attempted to fill the legal gap in personal data protection, such as the Regulation of the Minister of Communication and Information Technology Number 20 of 2016 on Personal Data Protection in Electronic Systems, which outlines the responsibilities of electronic system organizers in managing personal data.[35] Some areas require non-electronic data processing, although the regulation exclusively covers electronic data management.

The growing number of data breaches and abuse of personal data, both domestically and internationally, raises awareness of the need for more

[30] Rina Shahriyani Shahrullah, Jihyun Park, and Irwansyah Irwansyah, "Examining Personal Data Protection Law of Indonesia and South Korea: The Privacy Rights Fulfilment," *Hasanuddin Law Review* 10, no. 1 (2024): 10.

[31] Dian Ekawati, Toto Tohir, and Susanto Susanto, "Optimization of Consumer Protection and Increase of Virtual Currency Trading in Indonesia: A Study on Financial Services Authority Regulation," *Al-Ishlah: Jurnal Ilmiah Hukum* 27, no. 1 (2024): 69.

[32] Tuti Khairani Harahap et al., "Pengantar Ilmu Hukum," *Penerbit Tahta Media* 11, no. 4 (2023): 192.

[33] Masitoh Indriani, "Perlindungan Privasi dan Data Pribadi Konsumen Daring Pada Online Marketplace System," *Justitia Jurnal Hukum* 1, no. 2 (2017): 98.

[34] Syifaun Nafisah, "Electronic Information and Transaction Law, a Means of Information Control in Libraries," *Jurnal Kajian Informasi & Perpustakaan* 11, no. 1 (2023): 67.

[35] Dewa Gede Sudika Mangku et al., "The personal data protection of internet users in Indonesia," *Journal of Southwest Jiaotong University* 56, no. 1 (2021): 221.

comprehensive and in-depth legislation.[36] The Indonesian government recognizes the need for comprehensive personal data regulation, inspired by international regulations like the General Data Protection Regulation (GDPR) in the European Union. Personal Data Protection Law No. 27 of 2022 was passed following this parliamentary procedure.[37]

Overall, this highlights that although Indonesia now has a more comprehensive personal data protection law with Law No. 27 of 2022, the major challenge ahead is the successful implementation of this legislation. The Indonesian legal system has traditionally struggled with enforcement, particularly in monitoring and enforcing personal data protection laws. To address this, the law also empowers government-appointed entities to oversee and regulate personal data protection and prosecute violations.

3.2. Indonesia's Personal Data Protection Law 2022 and Its Challenges

Law No. 27 of 2022 updates Indonesia's personal data protection laws. First, this legislation clearly defines personal data. Law No. 27 of 2022 updates Indonesia's personal data protection laws. This legislation clearly defines personal data and categorizes it into two groups: specific and general.[38] Specific personal data refers to sensitive data that, if mishandled, could have significant repercussions. These include information such as health records, biometric data, genetic data, sexual orientation, political views, child-related data, and criminal records. Meanwhile, general personal data encompasses less sensitive information, such as names, genders, marital statuses, and religious affiliations. The distinction between these categories aims to provide varying levels of protection, with stricter safeguards applied to sensitive personal data to prevent misuse and protect individual rights.[39]

Sensitive personal data includes health, biometric, genetic, criminal, and child data, while general personal data comprises name, gender, religion, and marital status.[40] Due to the heightened risks of abuse, sensitive data requires tighter security. Law No. 27 of 2022 also defines and protects data subjects. Data subjects

[36] Oluwatosin Reis et al., "Privacy law challenges in the digital age: a global review of legislation and enforcement," *International Journal of Applied Research in Social Sciences* 6, no. 1 (2024): 78.

[37] Muhammad Deckri Algamar and Noriswadi Ismail, "Data Subject Access Request: What Indonesia Can Learn and Operationalise in 2024?," *Journal of Central Banking Law and Institutions* 2, no. 3 (2023): 499.

[38] Acep Rohendi and Dona Budi Kharisma, "Personal Data Protection in Fintech: A Case Study from Indonesia," *Journal of Infrastructure, Policy and Development* 8, no. 7 (2024): 4158.

[39] Ninne Zahara Silviani et al., "Personal Data Protection in Private Sector Electronic Systems for Businesses: Indonesia vs. South Korea," *Jurnal Hukum dan Peradilan* 12, no. 3 (2023): 528.

[40] Endah Fuji Astuti et al., "Assessing Indonesian MSMEs' Awareness of Personal Data Protection by PDP Law and ISO/IEC 27001: 2013," *International Journal of Safety & Security Engineering* 14, no. 5 (2024), 1655.

have the right to know who collects their data, why it is collected, and how it will be maintained and preserved. They may also request access to their data, correct errors, and remove irrelevant information. These rights provide individuals with more control over their personal data and ensure transparency and accountability in data usage.[41]

Data controllers, who collect and handle personal data, must also comply with Law No. 27 of 2022. They must obtain valid consent from data subjects and use the data solely for specified purposes. Data controllers are also required to prevent unauthorized access, disclosure, and alteration of personal data. To prevent data leaks, data controllers must establish a robust security system and notify data subjects if their data is compromised.[42] This legislation also governs the transfer of personal data both domestically and internationally, requiring data controllers to ensure that the recipient provides a comparable or greater level of protection. Law No. 27 of 2022 applies to data controllers in the commercial sector, governmental authorities, and foreign organizations that handle personal data in Indonesia. This reflects the Indonesian government's commitment to standardizing personal data management and protection across both public and commercial institutions.[43]

Law Number 27 of 2022 protects personal data, ensuring digital privacy rights. This regulation was created in response to the increasing processing of personal data in both the commercial and public sectors, as well as the risk of data abuse leading to breaches of privacy rights. Law No. 27 of 2022 provides a clear and comprehensive legal framework that was not fully addressed by other laws and regulations, such as the Law No. 11 of 2008 on Information and Electronic Transactions (ITE Law).[44]

Several major provisions in this law safeguard personal data. Article 1 defines "personal data" as data that may identify a person either electronically or non-electronically.[45] Article 3 states that any processing of personal data must protect

[41] Ahdiana Yuni Lestari et al., "Improving Healthcare Patient Data Security: An Integrated Framework Model for Electronic Health Records from A Legal Perspective," *Law Reform* 20, no. 2 (2022): 341.

[42] Nafila Andriana Putri, "Doxing Untuk Malicious Purposes vs Doxing Untuk Political Purposes: Urgensi Pengklasifikasian Ancaman Hukuman Bagi Para Pelaku Doxing Dalam Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi," *Padjadjaran Law Review* 11, no. 3 (2023): 54.

[43] Zlatan Morić et al., "Protection of Personal Data in the Context of E-Commerce," *Journal of cybersecurity and privacy* 4, no. 3 (2024): 748.

[44] Dian Purwaningrum Soemitro, Muhammad Arvin Wicaksono, and Nur Aini Putri, "Penal Provisions in the Personal Data Protection Law: A Comparative Legal Study between Indonesia and Singapore," *SIGn Jurnal Hukum* 5, no. 1 (2023): 106.

[45] Sinta Dewi Rosadi, Tasya Safiranita Ramli, and Rizki Fauzi, "Utilization of Non-Fungible Token and Regulatory Challenges in Indonesia: Aspects of Copyright Law," *Journal of Intellectual Property Rights (JIPR)* 29, no. 5 (2024): 114.

the data subjects' rights and ensure data security. Article 4 categorizes personal data into general and particular categories. Sensitive data, including health, biometric, genetic, and criminal records, must be protected due to the potential risks of abuse and loss. General data includes full name, gender, and religion. The rights of data subjects are outlined in Chapter IV, Articles 5–15. These rights include the right to obtain information about data processing (Article 5), the right to correct errors or inaccuracies (Article 6), the right to erase data (Article 8), and the right to withdraw consent (Article 9). However, Article 15 allows exceptions to certain rights for defense, national security, and law enforcement purposes, emphasizing the balance between individual rights and public interests.[46]

Personal data processors and controllers are subject to stringent requirements under Law No. 27 of 2022. Data controllers must comply with data processing laws, protect personal data from unauthorized access or disclosure, and notify data subjects in the event of data protection failures (Article 46). Data controllers are also required to verify data accuracy (Article 29) and destroy data after the retention period has expired (Article 43). This statute explicitly regulates both administrative and criminal sanctions. Personal data abuses are criminalized in Chapter 14, Articles 67–73. Unauthorized collection or use of personal data may result in a five-year prison sentence and fines of up to five billion rupiah (Article 67). Falsifying personal data may result in a six-year prison sentence and fines of up to six billion rupiah (Article 68). The legislation also includes provisions for the seizure of illicit earnings and corporate fines of up to 10 times the individual fine (Article 70).

This denotes that the effectiveness of personal data protection in Indonesia and the consistency of law enforcement are key challenges in implementing Law Number 27 of 2022 on Personal Data Protection. While this legislation is a significant step forward, its implementation faces technological and regulatory hurdles.[47] One of the initial challenges is the inadequate public understanding of personal data rights. Many Indonesians are not fully aware of data privacy or their rights as data subjects under Articles 5 to 15 of Law No. 27 of 2022.[48]

One of the main challenges of the Personal Data Protection (PDP) Law is the implementation of the duties of data controllers and processors. Articles 20 to 39 require data controllers and processors to secure and accurately handle personal data. However, not all organizations have the necessary infrastructure to comply.

---

[46] Jamal Wiwoho, Umi Khaerah Pati, and Anugrah Muhtarom Pratama, "Reciprocal Data Portability to Foster Financial Services Competition in the Open Banking System Era," *Yustisia* 13, no. 2 (2024): 84.

[47] Mohammad Fadel Roihan Ba'abud and Dodik Setiawan Nur Heriyanto, "Application of The Principles of Extraterritorial Jurisdiction Towards Personal Data Breach Committed Cross-Country Borders," *Uti Possidetis: Journal of International Law* 5, no. 1 (2024): 65.

[48] Kevin Raihan and Sinta Dewi Rosadi, "Have AI-Enhanced Telemedicines in Indonesia Adopted the Principles of Personal Data Protection?," *Yustisia* 13, no. 2 (2024): 97.

Many data controllers, particularly in the private sector and among small organizations, lack adequate legal security mechanisms and internal processes. As a result, personal data remains vulnerable to loss or exploitation, as demonstrated by numerous data breaches in both Indonesian government and private sector organizations.[49]

In this regard, supervision and law enforcement present significant challenges. Articles 58 to 60 of Law No. 27 of 2022 establish a separate institution for oversight, administrative law enforcement, and conflict resolution. The success of this institution depends on having proper infrastructure and sufficient personnel resources. Limited supervisory capacity and a shortage of personal data protection officers could hinder effective law enforcement. Supervisory institutions must be granted substantial authority and must coordinate with law enforcement to address major infractions.[50] However, proving personal data breaches is challenging, especially when they involve complex digital technologies. Under Article 64 of Law No. 27 of 2022, arbitration, courts, or other alternative conflict resolution mechanisms may address personal data disputes. The main difficulty lies in legally proving a personal data breach, especially when the data is exploited in a digital environment involving multiple parties, including those outside of Indonesia.[51]

International collaboration is also impacted, as data controllers outside of Indonesia may not have data protection standards comparable to those outlined in Law No. 27 of 2022, as stated in Article 56.[52] The effectiveness of criminal penalties is also a matter of debate. The criminal provisions for breaches of personal data privacy in Chapter 14 include imprisonment of up to five years and/or fines of up to five billion rupiah for individuals, with even harsher penalties for businesses. But how effective are these punishments in preventing violations? While heavy penalties may deter some, many organizations opt to pay fines rather than invest significantly in data protection measures. Therefore, the imposition of fines should

[49] Indra Rahmatullah, Pujiyono Suwadi, and Hari Purwadi, "Legal Reform of Zakat Management Based on Personal Data Protection Law in Indonesia," *Mazahib* 23, no. 1 (2024): 211.

[50] Pujiyono Suwadi et al., "Legal comparison of the use of telemedicine between Indonesia and the United States," *International Journal of Human Rights in Healthcare* 17, no. 3 (2022): 321.

[51] Naufal Mahira Dewantoro and M. H. Dian Alan Setiawan SH, "Penegakan Hukum Kejahatan Siber Berbasis Phising Dalam Bentuk Application Package Kit (APK) Berdasarkan Undang-Undang Informasi Dan Transaksi Elektronik," in *Bandung Conference Series: Law Studies* 3, no. 3 (2023): 896.

[52] Yogesh K. Dwivedi et al., "Metaverse beyond the hype: Multidisciplinary perspectives on emerging challenges, opportunities, and agenda for research, practice and policy," *International journal of information management* 66, no.4 (2022): 102542.

be balanced with incentives for companies and organizations to invest in improving data security.[53]

3.3. Personal Data Protection Mechanism under Global Standards: International Comparisons

Indonesia's PDP legislation provides a robust data protection structure, however its execution is difficult. The knowledge and preparedness of public and private bodies to comply with this regulation is a major problem. Indonesian SMEs may lack the infrastructure and ability to secure data. Private sector data controllers must balance legal duties with cost management, particularly when purchasing advanced data security solutions. The possibility for data breaches remains significant since government entities that function as data controllers are not completely equipped to execute this law's security criteria.[54]

On top of capacity difficulties, personal data protection breaches must be monitored and enforced. An entity overseeing and enforcing these restrictions is established by Law No. 27 of 2022, but its performance depends on proper resource support. Unsupervised data controllers may merely comply with the regulations nominally but not really implement data protection measures. This may lead to recurring data breaches or third-party exploitation of personal data.[55]

Law enforcement suffers evidential challenges, particularly when infractions occur online. Complex digital technology makes it hard for authorities to gather evidence and prove offenders' guilt.[56] This legislation is more difficult when infractions involve companies beyond Indonesia's jurisdiction. Article 62 requires effective international cooperation to quickly and equitably resolve cross-border infringement. This demands good cooperation between Indonesia and other nations and compliance with international norms like the EU's General Data Protection Regulation (GDPR).[57]

It is crucial to note that each nation has a distinct approach to personal data protection based on legal, social, and economic considerations when comparing

[53] Rudi Natamiharja and Ikhsan Setiawan, "Guarding Privacy in the Digital Age: A Comparative Analysis of Data Protection Strategies in Indonesia and France," *Jambe Law Journal* 7, no. 1 (2024): 233.

[54] Rina Arum Prastyanti and Ridhima Sharma, "Establishing Consumer Trust Through Data Protection Law as a Competitive Advantage in Indonesia and India," *Journal of Human Rights, Culture and Legal System* 4, no. 2 (2024): 229.

[55] Beni Kharisma Arrasuli and Khairul Fahmi, "Perlindungan Hukum Positif Indonesia Terhadap Kejahatan Penyalahgunaan Data Pribadi," *Unes Journal of Swara Justisia* 7, no. 2 (2023): 236.

[56] Junaidi, Pujiono, and Rozlinda Mohamed Fadzil, "Legal Reform of Artificial Intelligence's Liability to Personal Data Perspectives of Progressive Legal Theory," *Journal of Law and Legal Reform* 5, no. 2 (2024): 599.

[57] Shahrullah, Park, and Irwansyah, "Examining Personal Data Protection Law," 12.

Indonesia to other ASEAN, Asian, and European countries. The newly approved Indonesian Law Number 27 of 2022 highlights the government's attempts to safeguard people' personal data. However, how this rule compares to Singapore, Japan, and the EU, which have the GDPR, warrants more study.

The Personal Data Protection Act (PDPA) was one of the first and most comprehensive personal data protection laws in South-east Asia when Singapore adopted it in 2012.[58] The Personal Data Protection Act (PDPA) protects personal data in a business environment and requires data subjects to permission before their data is collected and processed, like Law No. 27 of 2022 in Indonesia. Singapore's Personal Data Protection Act (PDPA) imposes substantial administrative penalties, up to $1 million for major violations, unlike Indonesia's. The Personal Data Protection Act (PDPA) is successful in preventing breaches because these fees typically push commercial enterprises to comply with data protection laws. In this situation, Indonesia must apply Law No. 27 of 2022's criminal and administrative punishments as confidently as Singapore.

Japanese legislation is also advanced thanks to the 2003 Act on the Protection of Personal Information (APPI), which has been updated multiple times to stay up with worldwide advances. This rule was tightened when Japan adopted international norms in accordance with the EU's GDPR, notably for cross-border data handling. Additional protection for data subjects when data is transmitted abroad is a significant aspect of the Act on the Protection of Personal Information (APPI). The Act on the Protection of Personal Information (APPI) I requires Japanese data controllers to guarantee that the target country provides similar data protection for cross-border data transfers.[59] Law No. 27 of 2022 has to be clarified to safeguard Indonesian residents' personal data sent overseas. Indonesia's Personal Data Protection Law's Article 56 regulates this, however the key problem is making the international cooperation framework effective. Compared to the 2018 EU General Data Protection Regulation (GDPR), Law No. 27 of 2022 is still in its early phases of enforcement and technological implementation.

The General Data Protection Regulation (GDPR) is one of the most extensive data protection laws in the world, particularly as it extends to non-EU organisations who handle European individuals' personal data. The General Data Protection Regulation (GDPR)'s wide rights to data subjects, including the right to be

[58] Benjamin Wong YongQuan, "Data Privacy Law in Singapore: The Personal Data Protection Act 2012," *International Data Privacy Law* 7, no. 4 (2017): 291.

[59] Soichiro Saeki, "Impact of the Amendments to the Act of the Protection of Personal Information to Global Health Research Conducted in Japanese Medical Facilities," *Journal of Epidemiology* 32, no. 9 (2022): 438.

forgotten and the right to view their data in full, are its most striking features.[60] Law No. 27 of 2022 in Indonesia gives data subjects the right to have their data deleted, but small data controllers may not understand how to comply with the standard.

In addition, the General Data Protection Regulation (GDPR) has harsh penalties that may exceed 4% of the infringing company's worldwide yearly sales, which puts a lot of pressure on multinational firms to comply. Each EU member state's Data Protection Authorities (DPAs) implement the General Data Protection Regulation (GDPR) and have levied considerable punishments on major firms.[61] Chapter 14 of Law No. 27 of 2022 in Indonesia specifies significant criminal and administrative sanctions, but the biggest challenge is how to ensure consistent and effective law enforcement for personal data breaches, especially when dealing with corporate entities with great financial power and resources[62].

Both the General Data Protection Regulation (GDPR) and Law No. 27 of 2022 emphasise consent as the legal basis for processing personal data and the need to secure sensitive data. The preparedness of the technical and legal infrastructure that facilitates legislation execution is a key distinction. In Indonesia, Law No. 27 of 2022 is still being implemented and needs infrastructural and supervisory institution upgrades. Europe has a sophisticated supervisory system built on cross-border collaboration.[63]

3.4. Securing the Implementation of Personal Data Protection in Indonesia

The challenges mentioned above highlight the urgency of efficiently implementing Law Number 27 of 2022, concerning Personal Data Protection, in Indonesia. This implementation must adopt an integrated legal, technical, institutional, and social approach. It should address issues related to infrastructural preparedness, law enforcement, and public awareness. Based on both international and Indonesian experiences, here are some recommendations and an in-depth analysis for implementing Law Number 27 of 2022.

---

[60] Eduard Fosch Villaronga, Peter Kieseberg, and Tiffany Li, "Humans Forget, Machines Remember: Artificial Intelligence and the Right to Be Forgotten," *Computer Law & Security Review* 34, no. 2 (2018): 161.

[61] Charles Raab and Ivan Szekely, "Data Protection Authorities and Information Technology," *Computer Law & Security Review* 33, no. 4 (2017): 227.

[62] Wardah Yuspin et al., "The Regulations of the Supervisory Officer Personal Data Protection-Based Accountability Principle," *Bestuur* 12, no. 1 (2024): 59.

[63] Faiz Rahman and Cora Kristin Mulyani, "Minimising Unnecessary Restrictions on Cross-Border Data Flows? Indonesia's Position and Challenges Post Personal Data Protection Act Enactment," *International Review of Law, Computers & Technology* 8, no. 2 (2024): 10.

Personal data protection awareness must be raised through public, industry, and educational efforts.[64] Data privacy rights are still poorly understood in Indonesia. Many people are unaware that their personal data could be exploited or commercialized without their consent, or that they have the right to view, update, or delete their data under Articles 5 to 15 of Law No. 27 of 2022. Therefore, the government and affiliated organizations must launch a comprehensive education campaign using both traditional and digital media. The government may collaborate with digital platforms, technology companies, and other commercial sectors to disseminate information in a way that is accessible to the public.[65] Additionally, the government must provide guidance and training to businesses, particularly SMEs, to ensure they understand how to comply with the Personal Data Protection Law, as many may not yet comprehend its requirements. Raising awareness among both data controllers and the public is expected to enhance compliance with the law.

Public education and socialization in this regard are essential. Low public understanding of data subject rights is a major issue in personal data protection.[66] Therefore, the government, related organizations, and the business sector must increase socialization of data subject rights under Law No. 27 of 2022.[67] Public campaigns on social media, seminars, and training sessions can raise awareness of data privacy and teach people how to protect their data. To educate younger generations for the digital age, schools should consider incorporating this topic into their curricula. Therefore, schools can also play a significant role by incorporating digital privacy topics into the curriculum, equipping younger generations with the knowledge they need to navigate the digital world safely. In addition, strengthening the capacity of supervisory and law enforcement institutions is critical. The strengthening of law enforcement must be implemented efficiently by reinforcing the supervisory organization specified in Articles 58 to 60 of Law No. 27 of 2022 in terms of infrastructure, human resources, and authority. This institution must be capable of supervising, enforcing, and quickly resolving personal data infractions. In the constantly evolving digital age, the government must provide this organization with the necessary resources to handle complex

[64] Sambhabi Patnaik et al., "Safeguarding Patient Privacy: Exploring Data Protection in E-Health Laws: A Cross-Country Analysis," *Eai Endorsed Transactions on Pervasive Health and Technology* 10, no. 3 (2024): 231.

[65] Muhammad Khaeruddin Hamsin et al., "Sharia E-Wallet: The Issue of Sharia Compliance and Data Protection," *Al-Manahij: Jurnal Kajian Hukum Islam* 17, no. 1 (2023): 61.

[66] Wardah Yuspin et al., "Personal data protection law in digital banking governance in Indonesia," *Studia Iuridica Lublinensia* 32, no. 1 (2023): 115.

[67] Ari Wibowo, Widya Alawiyah, and Azriadi, "The Importance of Personal Data Protection in Indonesia's Economic Development," *Cogent Social Sciences* 10, no. 1 (2024): 2306751.

personal data matters. To effectively handle cases, police and prosecutors require specialized training on personal data crimes.[68]

Moreover, enhancing technology infrastructure for data security is a priority. For instance, data security should be improved by both public and private data controllers. The government may encourage data controllers to invest in data encryption, dual authentication, and security assessments.[69] Data controllers must use encryption, network security, and access control to safeguard personal data under Law No. 27 of 2022. As required by Law No. 27 of 2022, data controllers must establish clear rules and processes for processing and storing personal data. The government may also offer financial incentives or rewards to corporations or organizations that adhere to strict data privacy regulations. The government may provide technical incentives to data controllers, particularly small enterprises, to ensure access to this technology. Companies that invest in data security technologies could receive government subsidies or tax benefits. The government should also encourage SMEs to adopt more affordable and accessible technology to comply with the Personal Data Protection Law.[70] However, the supervisory agency must have advanced technology to audit and monitor data controllers. AI and blockchain can track data transfers more accurately, making breaches and infractions easier to detect. Regulatory Technology (RegTech) can also automate monitoring and provide real-time compliance data to help organizations meet regulations. [71]

At the same time, the regulation and enforcement of sanctions need to be strengthened. Although the fines under Law No. 27 of 2022 are harsh, their enforcement is challenging. The government must apply the administrative and criminal punishments outlined in Chapter 14 uniformly and equitably. Supervisory institutions should also be given more authority to penalize offenders, both individuals and organizations. Strengthening supervisory and law enforcement agencies is crucial for the effective implementation of Law No. 27 of 2022. The supervisory entity created under Article 58 of the Personal Data Protection Law must have adequate independence, authority, and competence to oversee data

[68] I Gusti Ngurah Parikesit Widiatedja and Neha Mishra, "Establishing an Independent Data Protection Authority in Indonesia: A Future–Forward Perspective," *International Review of Law, Computers & Technology* 37, no. 3 (2023): 186.

[69] Sinta Dewi Rosadi et al., "Indonesia's personal data protection bill, 2020: does it meet the needs of the new digital economy?," *International Review of Law, Computers & Technology* 37, no. 1 (2023): 85.

[70] Fithriatus Shalihah and Roos Niza Mohd Shariff, "Identifying Barriers to Data Protection and Investor Privacy in Equity Crowdfunding: Experiences from Indonesia and Malaysia, *UUM Journal of Legal Studies* 13, no. 2 (2022): 120.

[71] Citi Rahmati Serfiyani et al., "Developers Data Protection in the Open-Source Application with the Copyleft License," *Lentera Hukum* 8, no. 1 (2021): 23.

controllers and processors.[72] In many underdeveloped nations, including Indonesia, weak supervision hampers the enforcement of legal measures against violations.[73]

To address this, supervisory institutions need real-time infrastructure to monitor data controller activities, as well as the ability to issue warnings, impose administrative penalties, and conduct thorough investigations into data breaches. This means the government should increase audits and inspections of data controllers, particularly in high-risk sectors such as banking, insurance, and e-commerce, to improve prevention.[74] Additionally, the agency must be capable of identifying and addressing infractions in digital channels, which are often complex and involve difficult-to-trace perpetrators. The European Union's experience with the General Data Protection Regulation (GDPR) demonstrates that successful implementation relies not only on strict regulations but also on the presence of Data Protection Authorities (DPAs) with the technical capabilities to enforce the law and engage in international cooperation. Indonesia should adopt this model by ensuring that its personal data supervisory body is equipped to handle both digital and cross-border data breaches effectively.[75]

Moreover, international collaboration is crucial. Due to globalization, data breaches often involve overseas parties. According to Article 62 of Law No. 27 of 2022, international cooperation must be enhanced.[76] Indonesia needs to collaborate with other countries and organizations to protect Indonesian citizens' personal data handled abroad. By partnering with nations that have strong data protection laws, such as those in the EU under the GDPR, Indonesia can exchange experiences and enforcement methods. International collaboration is essential for the effective implementation of Law No. 27 of 2022. In a globalized environment, companies outside Indonesia often handle personal data. However, different nations have varying data protection regulations, which makes law enforcement challenging. Cross-border data transfers are regulated under Articles 56 to 62 of the Personal Data Protection Law, but greater international cooperation agreements are still needed. Indonesia should partner with countries that have strong data protection laws, such as the EU with its GDPR, Japan with its APPI,

[72] Rahmi Ayunda, "Personal Data Protection to E-Commerce Consumer: What Are the Legal Challenges and Certainties?," *LAW REFORM* 18, no. 2 (2022): 88.

[73] Giosita Kumalaratri and Yunanto Yunanto, "Urgency of The Personal Data Protection Bill on Privacy Rights in Indonesia," *Jurnal Hukum* 37, no. 1 (2021): 7.

[74] Russel Butarbutar, "Personal Data Protection in P2P Lending: What Indonesia Should Learn from Malaysia?," *Pertanika Journal of Social Sciences and Humanities* 28, no. 3 (2020): 2302.

[75] Fitri Adelia, "Peran Otoritas Jasa Keuangan Atas Perlindungan Data Pribadi Konsumen Fintech Lending," *Dinamika* 27, no. 21 (2022): 1997.

[76] Muhammad Saiful Rizal, Yuliati Yuliati, and Siti Hamidah, "Perlindungan Hukum Atas Data Pribadi Bagi Konsumen Dalam Klausula Eksonerasi Transportasi Online," *Legality: Jurnal Ilmiah Hukum* 27, no. 1 (2019): 77.

and Singapore with its PDPA. This collaboration is vital to safeguard Indonesian citizens' personal data processed overseas and to promote global data protection standards. By participating in international data protection forums like the G20 or ASEAN, Indonesia can enhance its local data protection laws and stay aligned with global developments.[77]

Additionally, there is a need to establish an efficient dispute resolution mechanism. Arbitration, courts, or other alternative conflict resolution agencies may resolve personal data issues under Article 64. However, this process must be more efficient and cost-effective for individuals. The government could support the creation of an online dispute resolution portal, enabling the public to quickly report personal data infractions. A more accessible dispute resolution process would allow the public to actively assert their rights and hold data controllers accountable for violations.[78]

Some also argue that incentives for data controllers who comply with the law should be introduced, in addition to punishments. The government could reward data controllers who adhere to Law No. 27 of 2022 by offering awards or accreditations to those with robust data security measures and a proven track record of protecting customers' personal data. These incentives would encourage improvements in data security while boosting the reputation and customer trust of compliant organizations punishments.

Chapter 14 of this Law governs criminal and administrative penalties for violations. Consistent implementation will determine the efficacy of these punishments. If penalties are only applied to significant instances and minor transgressions are overlooked, the public and data controllers will receive a weak message. Therefore, robust law enforcement is needed for data breaches by both large and small enterprises to avoid discrimination in punishments. Law enforcement must also ensure procedural fairness. Data violators must have the right to defend themselves and undergo a fair legal process, so that fines can effectively push corporations to educate themselves and promote better data security. The EU's experience with the General Data Protection Regulation (GDPR) shows that substantial penalties are often a major driver of compliance, but clear audit and enforcement systems are also crucial to ensuring adherence to the law.[79]

---

[77] Moh Hamzah Hisbulloh, "Urgensi Rancangan Undang-Undang (RUU) Perlindungan Data Pribadi," *Jurnal Hukum* 37, no. 2 (2021): 87.

[78] Ahmad Mahardika Mahardika, "Desain Ideal Pembentukan Otoritas Independen Perlindungan Data Pribadi Dalam Sistem Ketatanegaraan Indonesia," *Jurnal Hukum* 37, no. 2 (2021): 61.

[79] Luh Anastasia Trisna Dewi, Ni Putu Suci Meinarni, and I. Dewa Gede Dana Sugama, "Analisis Ekonomi Terhadap Hukum Dalam Kegagalan Perlindungan Data Pribadi Pengguna E-Commerce," *Jurnal Ius Kajian Hukum dan Keadilan* 9, no. 3 (2021): 2231.

Overall, the findings demonstrate that Law No. 27 of 2022 must be implemented holistically, encompassing institutional strengthening, public education, technological development, tough law enforcement, and tighter international collaboration. These initiatives are intended to create a secure digital environment in Indonesia where data controllers are accountable and data privacy is protected.

4. Conclusion

The findings reveal that Law Number 27 of 2022 provides a robust legal framework for safeguarding personal data in Indonesia; however, its execution remains challenging. This legislation protects data subjects' rights and defines data controllers' duties, but low public awareness and weak control and law enforcement powers hinder its implementation. Despite its severity, the criminal punishments outlined in Law Number 27 of 2022 require consistent application and effective technological support to prevent violations. This research suggests strengthening regulatory institutions, improving public education and socialization on personal data protection, and enhancing data controller security technologies. Further study is needed to assess the long-term efficacy of this law, particularly regarding international collaboration in cross-border data protection and companies' willingness to comply. The future effectiveness of this law depends on strict and impartial law enforcement.

In conclusion, Indonesia's Law Number 27 of 2022 on Personal Data Protection represents a significant step forward in safeguarding personal data and addressing violations in an era of rapid technological advancement. The law establishes a robust framework for data protection by introducing criminal sanctions for breaches, which serve as a deterrent to potential violators. However, the evaluation reveals that the efficacy of these sanctions is contingent upon consistent enforcement, public awareness, and judicial readiness to handle data protection cases. While the criminal provisions provide a strong legal basis, gaps remain in ensuring that sanctions are effectively applied and that victims of data breaches are adequately compensated. To enhance its effectiveness, the law must be supported by clear regulatory guidelines, capacity-building measures for law enforcement, and public education initiatives to foster a culture of data privacy. Strengthening these elements will help Indonesia achieve its goal of comprehensive personal data protection and align with global standards in digital rights and privacy.

References

Adelia, Fitri. "Peran Otoritas Jasa Keuangan Atas Perlindungan Data Pribadi Konsumen Fintech Lending." *Dinamika* 27, no. 21 (2022): 3142-3157.

Algamar, Muhammad Deckri, and Noriswadi Ismail. "Data Subject Access Request: What Indonesia Can Learn and Operationalise In 2024?" *Journal of Central Banking Law and Institutions* 2, no. 3 (2023): 481-512.

Astuti, Endah Fuji, Achmad Nizar Hidayanto, Sabila Nurwardani, and Ailsa Zayyan Salsabila. "Assessing Indonesian MSMEs' Awareness of Personal Data Protection by PDP Law and ISO/IEC 27001: 2013." *International Journal of Safety & Security Engineering* 14, no. 5 (2024). 1559–1567.

Ba'abud, Mohammad Fadel Roihan, and Dodik Setiawan Nur Heriyanto. "Application of The Principles of Extraterritorial Jurisdiction Towards Personal Data Breach Committed Cross-Country Borders."*Uti Possidetis: Journal of International Law* 5, no. 1 (2024): 106-137.

Benn, Stanley I. "Privacy, freedom, and respect for persons." In *Privacy and personality*, pp. 1-26. Routledge, 2017.

Capurro, Rafael, Michael Eldred, and Daniel Nagel. *Digital Whoness: Identity, Privacy and Freedom in the Cyberworld*. Boston: Walter de Gruyter, 2013.

Cohen, Julie E. 'What Privacy Is For". *Harvard Law Review* 126 (2013): 1904.

Dewantoro, Naufal Mahira, and M. H. Dian Alan Setiawan SH. "Penegakan Hukum Kejahatan Siber Berbasis Phising Dalam Bentuk Application Package Kit (APK) Berdasarkan Undang-Undang Informasi Dan Transaksi Elektronik." In *Bandung Conference Series: Law Studies*, 3:892–900, 2023.

Dewi, Luh Anastasia Trisna, Ni Putu Suci Meinarni, and I. Dewa Gede Dana Sugama. "Analisis Ekonomi Terhadap Hukum Dalam Kegagalan Perlindungan Data Pribadi Pengguna E-Commerce." *Jurnal IUS Kajian Hukum dan Keadilan* 9, no. 3 (2021): 2231-2245.

Ekawati, Dian, Toto Tohir, and Susanto Susanto. "Optimization of Consumer Protection and Increase of Virtual Currency Trading in Indonesia: A Study on Financial Services Authority Regulation." *Al-Ishlah: Jurnal Ilmiah Hukum* 27, no. 1 (2024): 60-75.

Fauzie, Muhamad Alfat. "Securing The Future: Indonesia Personal Data Protection Law and It's Implication for Internet of Things (IOT) Data Privacy." *Sriwijaya Crimen and Legal Studies* 2, no. 1 (2024): 12-25.

Firmansyah, Muhammad Rizieq. "Perlindungan Data Pribadi Dalam Transaksi Elektronik Pra dan Pasca UU Nomor 27 Tahun 2022." Bachelor Thesis, Fakultas Syariah dan Hukum UIN Syarif Hidayatullah Jakarta, 2023. https://repository.uinjkt.ac.id/dspace/handle/123456789/76415.

Gurria, Angel. "OECD Employment Outlook 2020: Worker Security and the Covid-19 CRISIS." *OECD Employment Outlook* 14, no. 5 (2020): 116-221.

Hamsin, Muhammad Khaeruddin, Abdul Halim, Rizaldy Anggriawan, and Hilda Lutfiani. "Sharia E-Wallet: The Issue of Sharia Compliance and Data Protection." *Al-Manahij: Jurnal Kajian Hukum Islam* 17, no. 1 (2023): 53-68.

Harahap, Tuti Khairani, Yuyut Prayuti, Nining Latianingsih, Amsari Damanik, Tiyas Maheni, Ida Farida, and Mohamad Hidayat Muhtar. "Pengantar Ilmu Hukum." *Penerbit Tahta Media* (2023).

Hisbulloh, Moh Hamzah. "Urgensi Rancangan Undang-Undang (RUU) Perlindungan Data Pribadi." *Jurnal Hukum* 37, no. 2 (2021): 119–33.

Hoofnagle, Chris Jay, Bart van der Sloot, and Frederik Zuiderveen Borgesius. "The European Union General Data Protection Regulation: What It Is and What It Means". *Information & Communications Technology Law* 28, no. 1 (2019): 65–98.

Indriani, Masitoh. "Perlindungan Privasi dan Data Pribadi Konsumen Daring Pada Online Marketplace System." *Justitia Jurnal Hukum* 1, no. 2 (2017): 98.

Junaidi, Pujiono, and Rozlinda Mohamed Fadzil. "Legal Reform of Artificial Intelligence's Liability to Personal Data Perspectives of Progressive Legal Theory." *Journal of Law and Legal Reform* 5, no. 2 (2024): 587–612.

Kharisma, Dona Budi, and Alvalerie Diakanza. "Patient Personal Data Protection: Comparing the Health-Care Regulations in Indonesia, Singapore and the European Union." *International Journal of Human Rights in Healthcare* 17, no. 2 (2024): 157–169.

Kumalaratri, Giosita, and Yunanto Yunanto. "Urgency of the Personal Data Protection Bill on Privacy Rights in Indonesia." *Jurnal Hukum* 37, no. 1 (2021): 1–13.

Land, Joy. "Cohen-Scali Saguès, Julie". *Encyclopedia of Jews in the Islamic World*, 2010.

Lestari, Ahdiana Yuni, Misran Misran, Trisno Raharjo, Muhammad Annas, Dinda Riskanita, and Adya Paramita Prabandari. "Improving Healthcare Patient Data Security: An Integrated Framework Model for Electronic Health Records from A Legal Perspective." *Law Reform* 20, no. 2 (2024): 329–52.

Lestari, Endang, and Rasji Rasji. "Legal Study on Personal Data Protection Based on Indonesian Legislation." *Awang Long Law Review* 6, no. 2 (2024): 471–77.

Li, He, Lu Yu, and Wu He. "The Impact of GDPR on Global Technology Development." *Journal of Global Information Technology Management* 22, no. 1 (2019): 1–6.

Mahardika, Ahmad Mahardika. "Desain Ideal Pembentukan Otoritas Independen Perlindungan Data Pribadi Dalam Sistem Ketatanegaraan Indonesia." *Jurnal Hukum* 37, no. 2 (2021): 101–18.

Mahmud Marzuki, Peter. *Penelitian Hukum*. Jakarta: Kencana Prenada Media Group, 2011.

Mangku, Dewa Gede Sudika, Ni Putu Rai Yuliartini, I. Nengah Suastika, and I. Gusti Made Arya Suta Wirawan. "The Personal Data Protection of Internet Users in Indonesia." *Journal of Southwest Jiaotong University* 56, no. 1 (2021): 221.

Manurung, Evelyn Angelita Pinondang. "The Right to Privacy Based on the Law of the Republic of Indonesia Number 27 of 2022." *Journal of Digital Law and Policy* 2, no. 3 (2023): 103–10.

Mayasari, Hanita. "A Examination on Personal Data Protection in Metaverse Technology in Indonesia: A Human Rights Perspective." *Journal of Law, Environmental and Justice* 1, no. 1 (2023): 64–85.

Morić, Zlatan, Vedran Dakic, Daniela Djekic, and Damir Regvart. "Protection of Personal Data in the Context of E-Commerce." *Journal of Cybersecurity and Privacy* 4, no. 3 (2024): 731–61.

Mubashwir Alam, A. K. M., Sagar Sharma, and Keke Chen. "SGX-MR: Regulating Dataflows for Protecting Access Patterns of Data-Intensive SGX Applications." *ArXiv e-prints* 7, no. 2 (2020): 2009.

Nababan, Tabitha Fransisca Romauli, and Shevanna Putri Cantiqa. "Mengoptimalkan Implementasi UU No. 27 Tahun 2022 Dengan Penetration Test Dan Vulnerability Assessment Pada Kasus Pembobolan Data Aplikasi Dana." *Jurnal Hukum, Politik dan Ilmu Sosial* 3, no. 3 (2024): 155–61.

Nafisah, Syifaun. "Electronic Information and Transaction Law, a Means of Information Control in Libraries." *Jurnal Kajian Informasi & Perpustakaan Vol* 11, no. 1 (2023): 57–76.

Natamiharja, Rudi, and Ikhsan Setiawan. "Guarding Privacy in the Digital Age: A Comparative Analysis of Data Protection Strategies in Indonesia and France." *Jambe Law Journal* 7, no. 1 (2024): 233–51.

Patnaik, Sambhabi, Kyvalya Garikapati, Lipsa Dash, Ramyani Bhattacharya, and Arpita Mohapatra. "Safeguarding Patient Privacy: Exploring Data Protection in E-Health Laws: A Cross-Country Analysis." *EAI Endorsed Transactions on Pervasive Health and Technology* 10 (2024); 298-239.

Prastyanti, Rina Arum, and Ridhima Sharma. "Establishing Consumer Trust Through Data Protection Law as a Competitive Advantage in Indonesia and India." *Journal of Human Rights, Culture and Legal System* 4, no. 2 (2024): 354–90.

Priskarini, Intan Audia, and Kukuh Tejomurti "The Role of The Financial Services Authority in The Legal Protection of Privacy Rights in Connection with Personal Data of Fintech Lending Debtor in Indonesia | Peran Otoritas Jasa Keuangan (OJK) dalam Perlindungan Hukum Hak Privasi atas Data Pribadi Konsumen Peminjam Fintech Lending di Indonesia." *Padjadjaran Jurnal Ilmu Hukum* 6, no. 3 (2019): 556–575.

Puluhulawa, Jufryanto, Mohamad Hidayat Muhtar, Mellisa Towadi, and Vifi Swarianata. "The Concept of Cyber Insurance as a Loss Guarantee on Data Protection Hacking in Indonesia." *Law, State and Telecommunications Review* 15, no. 2 (2023): 132–45.

Putra, Tegar Islami, Akbar Jihadul Islam, and Abdullah Mufti Abdul Rahman. "Integrating Islamic Laws into Indonesian Data Protection Laws: An Analysis of Regulatory Landscape and Ethical Considerations." *Contemporary Issues on Interfaith Law and Society* 3, no. 1 (2024): 85–118.

Putri, Nafila Andriana. "Doxing Untuk Malicious Purposes vs Doxing Untuk Political Purposes: Urgensi Pengklasifikasian Ancaman Hukuman Bagi Para Pelaku Doxing Dalam Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi." *Padjadjaran Law Review* 11, no. 1 (2023): 102–13.

Raab, Charles, and Ivan Szekely. "Data Protection Authorities and Information Technology." *Computer Law & Security Review* 33, no. 4 (2017): 421–33.

Rahman, Faiz, and Cora Kristin Mulyani. "Minimising Unnecessary Restrictions on Cross-Border Data Flows? Indonesia's Position and Challenges Post Personal Data Protection Act Enactment." *International Review of Law, Computers & Technology* 0, no. 0 (n.d.): 1–20.

Rahmatullah, Indra, Pujiyono Suwadi, and Hari Purwadi. "Legal Reform of Zakat Management Based on Personal Data Protection Law in Indonesia." *Mazahib* 23, no. 1 (2024): 199–236.

Raihan, Kevin, and Sinta Dewi Rosadi. "Have AI-Enhanced Telemedicines in Indonesia Adopted the Principles of Personal Data Protection?" *Yustisia* 13, no. 2 (2024): 151–67.

Reis, Oluwatosin, Nkechi Emmanuella Eneh, Benedicta Ehimuan, Anthony Anyanwu, Temidayo Olorunsogo, and Temitayo Oluwaseun Abrahams. "Privacy Law Challenges in The Digital Age: A Global Review of Legislation and Enforcement." *International Journal of Applied Research in Social Sciences* 6, no. 1 (2024): 73–88.

Rizal, Muhammad Saiful, Yuliati Yuliati, and Siti Hamidah. "Perlindungan Hukum Atas Data Pribadi Bagi Konsumen Dalam Klausula Eksonerasi Transportasi Online." *Legality: Jurnal Ilmiah Hukum* 27, no. 1 (2019): 68–82.

Rohendi, Acep, and Dona Budi Kharisma. "Personal Data Protection in Fintech: A Case Study from Indonesia." *Journal of Infrastructure, Policy and Development* 8, no. 7 (2024): 4158.

Rosadi, Sinta Dewi, Andreas Noviandika, Robert Walters, and Firsta Rahadatul Aisy. "Indonesia's Personal Data Protection Bill, 2020: Does It Meet the Needs of the New Digital Economy?" *International Review of Law, Computers & Technology* 37, no. 1 (2023): 78–90.

Rosadi, Sinta Dewi, Tasya Safiranita Ramli, and Rizki Fauzi. "Utilization of Non-Fungible Token and Regulatory Challenges in Indonesia: Aspects of Copyright Law." *Journal of Intellectual Property Rights (JIPR)* 29, no. 5 (2024): 389–95.

Saeki, Soichiro. "Impact of the Amendments to the Act of the Protection of Personal Information to Global Health Research Conducted in Japanese Medical Facilities." *Journal of Epidemiology* 32, no. 9 (2022): 438–438.

Serfiyani, Citi Rahmati, Cita Yustisia Serfiyani, Iswi Hariyani, and Devina Tharifah Arsari. "Developers Data Protection in the Open-Source Application with the Copyleft License." *Lentera Hukum* 8 (2021): 23.

Shahrullah, Rina Shahriyani, Jihyun Park, and Irwansyah Irwansyah. "Examining Personal Data Protection Law of Indonesia and South Korea: The Privacy Rights Fulfilment." *Hasanuddin Law Review* 10, no. 1 (2024): 1–20.

Shalihah, Fithriatus, and Roos Niza Mohd Shariff. "Identifying Barriers to Data Protection and Investor Privacy in Equity Crowdfunding: Experiences From Indonesia And Malaysia." *UUM Journal of Legal Studies* 13, no. 2 (2022): 215–42.

Silvi, Ferina Widyawati Ayu, and Anom Wahyu Asmorojati. "The Urgency of Establishing a Special Agency of Personal Data Protection and Supervision to Ensure the Indonesian Citizens' Privacy Rights." *Borobudur Law Review* 4, no. 2 (2022): 110–22.

Silviani, Ninne Zahara, Rina Shahriyani Shahrullah, Vanessa Riarta Atmaja, and Park Ji Hyun. "Personal Data Protection in Private Sector Electronic Systems for Businesses: Indonesia vs. South Korea." *Jurnal Hukum Dan Peradilan* 12, no. 3 (2023): 517–46.

Simbolon, Valentina Ancillia, and Vishnu Juwono. "Comparative Review of Personal Data Protection Policy in Indonesia and The European Union General Data Protection Regulation." *Publik (Jurnal Ilmu Administrasi)* 11, no. 2 (2022): 178–90.

Singer, Joseph William. Legal Realism Now. *California Law Review* 76 (1988): 465-179.

Soemitro, Dian Purwaningrum, Muhammad Arvin Wicaksono, and Nur Aini Putri. "Penal Provisions in the Personal Data Protection Law: A Comparative Legal Study between Indonesia and Singapore." *SIGn Jurnal Hukum* 5, no. 1 (2023): 155–67.

Sudarwanto, Al Sentot, and Dona Budi Budi Kharisma. "Comparative Study of Personal Data Protection Regulations in Indonesia, Hong Kong and Malaysia." *Journal of Financial Crime* 29, no. 4 (2021): 1443–57.

Suwadi, Pujiyono, Priscilla Wresty Ayuningtyas, Shintya Yulfa Septiningrum, and Reda Manthovani. "Legal Comparison of the Use of Telemedicine between Indonesia and the United States." *International Journal of Human Rights in Healthcare* 17, no. 3 (2022): 315–29.

Goldstein, Tom. *Killing the Messenger: 100 Years of Media Criticism*. Columbia University Press, 2019.

Tribunnews.com. "Akademisi Sebut Perlindungan Data di RI Butuh Reformasi, Singgung Kebocoran Data e-KTP." Tribunnews.com, 26 December 2024. https://www.tribunnews.com/nasional/2024/12/19/akademisi-sebut-perlindungan-data-di-ri-butuh-reformasi-singgung-kebocoran-data-e-ktp.

Villaronga, Eduard Fosch, Peter Kieseberg, and Tiffany Li. "Humans Forget, Machines Remember: Artificial Intelligence and the Right to Be Forgotten." *Computer Law & Security Review* 34, no. 2 (2018): 304–13.

Voigt, Paul, and Axel Von Dem Bussche. *The EU General Data Protection Regulation (GDPR)*. Cham: Springer International Publishing, 2017.

Wibowo, Ari, Widya Alawiyah, and Azriadi. "The Importance of Personal Data Protection in Indonesia's Economic Development." *Cogent Social Sciences* 10, no. 1 (2024): 2306751.

Widiatedja, I Gusti Ngurah Parikesit, and Neha Mishra. "Establishing an Independent Data Protection Authority in Indonesia: A Future–Forward Perspective." *International Review of Law, Computers & Technology* 37, no. 3 (2023): 252–73.

Wiwoho, Jamal, Umi Khaerah Pati, and Anugrah Muhtarom Pratama. "Reciprocal Data Portability to Foster Financial Services Competition in the Open Banking System Era." *Yustisia* 13, no. 2 (2024): 134–50.

Wong Yong Quan, Benjamin. "Data Privacy Law in Singapore: The Personal Data Protection Act 2012." *International Data Privacy Law* 7, no. 4 (2017): 287–302.

Yusliwidaka, Arnanda, Muhammad Ardhi Razaq Abqa, and Khansadhia Afifah Wardana. "A Discourse of Personal Data Protection: How Indonesia Responsible under Domestic and International Law?" *Pandecta Research Law Journal* 19, no. 2 (2024): 173–202.

Yuspin, Wardah, Kelik Wardiono, Aditya Nurrahman, and Arief Budiono. "Personal Data Protection Law in Digital Banking Governance in Indonesia." *Studia Iuridica Lublinensia* 32, no. 1 (2023): 99–130.

Yuspin, Wardah, Trisha Rajput, Abhinayan Basu Bal, Kelik Wardiono, and Absori Absori. "The Regulations of the Supervisory Officer Personal Data Protection-Based Accountability Principle." *Bestuur* 12, no. 1 (2024): 49–68.