INTERNATIONAL JOURNAL OF JUDICIAL LAW

The Urgency and Challenges of Legal Protection of Personal Data in Indonesia

I Gusti Ngurah Putu Alit Putra [1*], I Gede Pasek Pramana [2]
[1-2] Faculty of Law Udayana University, Indonesia

* Corresponding Author: **I Gusti Ngurah Alit Putra**

Article Info

ISSN (online): 2583-6536
Volume: 05
Issue: 01
Received: 16-11-2025
Accepted: 18-12-2025
Published: 20-01-2026
Page No: 26-28

Abstract
The rapid development of information technology has had a significant impact on various aspects of life, including the protection of personal data. In Indonesia, issues concerning personal data protection have attracted increasing attention amid the rising number of data breach incidents and the misuse of personal information. This study aims to explore Indonesia's existing legal framework for personal data protection, identify the challenges encountered, and propose solutions to enhance its protection. The findings indicate that although Indonesia has enacted regulations governing personal data, their implementation and enforcement continue to face various obstacles. Strengthening public awareness, technological infrastructure, and cooperation among relevant stakeholders is therefore essential to ensure more effective personal data protection.

DOI: https://doi.org/10.54660/IJJL.2026.5.1.26-28

Keywords: Personal Data, Legal Protection, Indonesia, Data Security, Legal Challenges

1. Introduction

1.1. Background

In the digital era, which is characterized by the rapid development of information and communication technology, personal data has developed into a strategic asset that has high economic and legal value. Personal data includes any data about an identified or identifiable individual, either directly or indirectly, such as name, address, identity number, telephone number, and financial information. The massive use of personal data in various sectors, such as electronic commerce, digital banking, healthcare, and government, increases the potential for data misuse if it is not accompanied by an adequate legal protection system. (Danrivanto Budhijanto, 2020) [1]

The collection, storage, processing, and dissemination of personal data that is not in accordance with the principles of privacy protection can have serious consequences, including identity theft, fraud, and violation of individual privacy rights. (Sinta Dewi Rosadi, 2020) [2], In a legal perspective, the protection of personal data is part of the protection of human rights, especially the right to a sense of security and the right to personal protection as stipulated in Article 28G paragraph (1) of the Constitution of the Republic of Indonesia in 1945. Therefore, the state has an obligation to ensure effective legal protection of the personal data of every citizen.

The issue of personal data protection in Indonesia is increasingly becoming a public concern along with the rampant cases of data leaks in recent years. One of the biggest cases occurred in 2020, when the personal data of more than 91 million users of the Tokopedia e-commerce platform was reportedly leaked and illegally traded on online forums. [5] The case raised public concerns about the security of personal data and showed the weak data protection system implemented by electronic system operators.

These various data leak incidents indicate that there are serious challenges in the legal protection of personal data in Indonesia, both from the aspects of regulation, law enforcement, supervisory institutions, and the awareness of business actors and the public. Although Indonesia already has Law Number 27 of 2022 concerning Personal Data Protection as the main legal umbrella, in practice there are still various obstacles in the implementation and enforcement of sanctions against personal data breaches.

(Edmon Makarim, 2022) [3]
Based on this description, the author is interested in further studying the challenges of legal protection of personal data in Indonesia, in order to assess the effectiveness of the existing legal framework and identify the obstacles faced in optimal personal data protection efforts. Based on the above problems, the author raised the title "The Urgency and Challenges of Legal Protection of Personal Data in Indonesia".

2. Research Methodology

The type of research used is Normative Juridical (Legal Research). Law in the normative sense is law as a norm, both related to justice that must be achieved (ius constituendum) and norms that have been realized as explicit instructions and that have been formulated in detail (ius constitutum) to ensure certainty and also norms that are included in the product of judges (j.u.dments) when the judge decides a case by considering the realization of the benefits and benefits for the person in the case. This research was carried out to solve the legal problems that arise. Data were obtained through literature review, legislative and regulatory analysis, and interviews with experts in the field of law and information technology. The analysis was carried out by examining various legal and practical aspects related to personal data protection in Indonesia. Data was obtained through literature review, analysis of laws and regulations in the field of law and information technology. Meanwhile, the results that will be achieved are in the form of prescriptions to answer the problems in this study.

3. Results and Discussion

3.1. Challenges in Personal Data Protection in Indonesia

Legal protection of personal data in Indonesia has basically gained a strong normative foundation through the ratification of Law Number 27 of 2022 concerning Personal Data Protection (UUPDP). However, the existence of these regulations does not necessarily guarantee effective personal data protection in practice. There are a number of fundamental challenges that need serious attention so that the legal objectives of personal data protection can be achieved optimally. (F Nabawi, 2023)
One of the main challenges in personal data protection in Indonesia is the lack of awareness and education on the importance of protecting personal data. Many individuals and organizations do not understand the risks associated with the collection and use of personal data, as well as how to protect it from misuse. Many small and medium-sized enterprises (SMEs) do not yet have adequate policies or procedures in place to protect their customers' personal data. This makes the personal data they manage vulnerable to leakage or misuse.
Inadequate technological infrastructure is also an obstacle to personal data protection in Indonesia. Many regions in Indonesia still do not have sufficient access to secure and reliable information technology. This makes it difficult to implement effective data security measures, especially in remote areas. In addition, many organizations are still using outdated technology systems and are vulnerable to cyberattacks. The lack of investment in data security technology makes many organizations unprepared to deal with threats to the personal data they manage. This inadequate infrastructure includes limitations in terms of encryption technology, intrusion detection, and other mechanisms needed to effectively protect personal data. (Erikha, ZA Hoesein, 2025) [7]
Although Indonesia already has several regulations governing the protection of personal data, law enforcement is still a major challenge. One of the main problems is the lack of coordination between the agencies responsible for law enforcement in the field of data security. This often leads to inconsistencies in law enforcement and non-uniform policies across different regions. In addition, there are still differences in interpretation of several provisions in the law that govern the protection of personal data. This can lead to legal uncertainty for companies and individuals seeking to comply with existing regulations. There needs to be further clarification and harmonization to ensure that regulations can be applied consistently and effectively.
Cybersecurity threats continue to evolve and become increasingly sophisticated. Cyberattacks targeting personal data can include hacking, phishing, ransomware, and other methods that are constantly evolving. Many organizations in Indonesia are still unprepared for this threat due to a lack of investment in security technology and low awareness of good security practices. (A Anggara, MRK Dinata, 2023) [6]
The protection of personal data requires close collaboration between governments, the private sector, and society. However, in Indonesia, this
cooperation is still not optimal. Many organizations do not share their information or experience in dealing with cyber threats, which can strengthen overall data protection efforts. In addition, there are limitations in terms of cross-sector collaboration that can affect the effectiveness of handling data leak incidents. Better collaboration is needed to create a stronger data protection ecosystem.

3.2. Legal Measures to Improve Personal Data Protection in Indonesia

Legal efforts to improve personal data protection in Indonesia must be carried out comprehensively and sustainably, involving regulatory, institutional, law enforcement, and increasing public legal awareness. Although Law Number 27 of 2022 concerning Personal Data Protection (PDP Law) has provided a strong legal foundation, the effectiveness of personal data protection is highly dependent on the implementation of these legal norms in practice.
Legal remedies can be carried out through strengthening regulations and improving implementing regulations. The PDP Law still requires further regulation through government regulations and regulations of supervisory institutions to elaborate on technical provisions, such as personal data processing mechanisms, data security standards, and procedures for reporting and handling data breaches. The preparation of clear and integrated implementing regulations is important to prevent multi-interpretation and ensure legal certainty for controllers and subjects of personal data. (E Yolanda, RR Hutabarat, 2023) [5]
Education and raising awareness about the importance of personal data protection should be a priority. Governments, educational institutions, and non- governmental organizations should work together to improve public understanding of the risks associated with the collection and use of personal data. Educational programs can include public campaigns, training, and workshops designed to raise awareness of best practices in protecting personal data.
Investment in technology infrastructure is key to improving personal data protection in Indonesia. Governments and the private sector must work together to ensure that all regions

have adequate access to secure and reliable information technology. This includes improving the internet network, providing advanced encryption technology, and developing more effective intrusion detection and prevention mechanisms. (Y Wibowo, IADP Wulan, 2025) [4]

In addition, organizations should be encouraged to regularly update their technology systems and adopt the latest technologies that can protect personal data from cyber threats. The existing legal framework needs to be strengthened and updated regularly to keep up with technological developments and cyber threats. The government must ensure that all regulations relevant to the protection of personal data are applied consistently and effectively across regions. This can be done by improving coordination between law enforcement agencies and providing sufficient resources for law enforcement. In addition, there needs to be an effort to harmonize regulations between the central and regional governments and clarify provisions that are still ambiguous to reduce legal uncertainty.

The use of modern security technologies such as data encryption, intrusion detection and prevention systems, and artificial intelligence (AI) technology can help protect personal data from cyber threats. Organizations should be encouraged to adopt these technologies and ensure that they have security systems that are up-to-date and compliant with the best standards.

Closer collaboration between governments, the private sector, and the public is key to creating a strong data protection ecosystem. Governments should facilitate cooperation between various parties to share information and experiences on cyber threats and best practices in protecting personal data. In addition, international collaboration is also important to deal with cyber threats that are cross-border. Indonesia should strengthen relations with other countries and participate in international forums focused on data security and privacy.

4. Conclusion

Personal data protection is a very important issue in this digital age, especially with the increasing number of incidents of data leaks and misuse of personal information. In Indonesia, although there are several legal frameworks governing the protection of personal data, there are still many challenges that must be overcome.

To improve the protection of personal data in Indonesia, there needs to be greater efforts in terms of education and awareness, improving technological infrastructure, strengthening the legal framework, adopting modern security technologies, and increasing collaboration between sectors. With these measures, Indonesia can build a stronger data protection ecosystem and ensure that citizens' personal data is well protected.

International collaboration is also important to deal with global cyber threats and ensure that Indonesia can adopt best practices in personal data protection. With a strong commitment from all parties, Indonesia can overcome the challenges in personal data protection and ensure that the privacy and security of personal data are well maintained in this digital era.

5. References

1. Danrivanto B. Hukum Data Pribadi di Indonesia. Bandung: Refika Aditama; 2020. p. 3.
2. Rosadi SD. Perlindungan Privasi dan Data Pribadi dalam Era Ekonomi Digital di Indonesia. J Veritas et Justitia. 2020;6(1):89.
3. Makarim E. Tantangan Penegakan Hukum Perlindungan Data Pribadi di Indonesia. J Hukum Pembang. 2022;52(2):312.
4. Wibowo Y, Wulan IADP, Ismiyanto I. Tinjauan yuridis tentang perlindungan data pribadi masyarakat pada era digitalisasi. J Penelit Serambi Hukum. 2025;18(01):1-6.
5. Yolanda E, Hutabarat RR. UrgensI lembaga pelindungan data pribadi di indonesia berdasarkan asas hukum responsif. J Syntax Literate. 2023;8(6).
6. Anggara A, Dinata MRK. Hacker bjorka: pihak yang berperan dalam mencegah kebocoran data. J Hukum Magnum Opus. 2023;6(1).
7. Erikha A, Hoesein ZA. Strategi pencegahan kebocoran data pribadi melalui peran Kominfo dan gerakan Siberkreasi dalam edukasi digital. J Retentum. 2025;4(1):48-64.
8. Nabawi F. Perlindungan Hukum Terhadap Konsumen yang Dirugikan dalam Transaksi Jual Beli Pada Situs Belanja Online Shopee [doctoral dissertation]. Yogyakarta: Universitas Islam Indonesia; [year unknown, likely ~2020s based on context].
9. Peraturan Pemerintah Republik Indonesia Nomor 18 Tahun 2021 tentang Peraturan Pelaksanaan Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana telah diubah dengan Undang-Undang Nomor 19 Tahun 2016. [or specific title if available; Pasal 1].
10. Kitab Undang-Undang Hukum Perdata (Burgerlijk Wetboek voor Indonesië). Pasal 500.
11. Undang-Undang Nomor 4 Tahun 1996 tentang Hak Tanggungan atas Tanah Beserta Benda-benda yang Berkaitan dengan Tanah. Pasal 1.
12. Undang-Undang Nomor 5 Tahun 1960 tentang Peraturan Dasar Pokok-Pokok Agraria. Pasal 3 dan 5.

How to Cite This Article

Putra IGNPAP, Pramana IGP. The urgency and challenges of legal protection of personal data in Indonesia. Int J Judic Law. 2026;5(1):26-28. doi:10.54660/IJJL.2026.5.1.26-28.