INTERNATIONAL CONFERENCE ON THE STATE, LAW, POLITICS & DEMOCRACY (ICON-SLPD)
P-ISSN : 2962-7109 E-ISSN : 3063-6957
https://openjournal.unpam.ac.id/index.php/ICon

International Conference On The State, Law, Politics & Democracy (ICON-SLPD)
Conference Proceedings 2025

LEGAL PROTECTION OF PERSONAL DATA CONFIDENTIALITY IN THE DIGITALIZATION ERA REVIEWED FROM LAW NUMBER 27 OF 2022 CONCERNING PERSONAL DATA PROTECTION

Diah Irianti PS[1], Herlina Basri[2]

[1] Faculty of Law, Pamulang University, Tangsel. E-mail: *dosen02430@unpam.ac.id*

[2] Faculty of Law, Pamulang University, Tangsel. *E-mail: dosen01956@unpam.ac.id*

Article

Received: Des 02, 2025; Reviewed: Jan 07, 2026; Accepted: Feb 09, 2026; Published: Feb 26, 2026

Abstract

Everyone has personal data. Personal data is inherent in every person and must be protected because it is essentially everyone's right to privacy. The right to privacy is a constitutional right of citizens as stipulated in the 1945 Constitution. Constitutional rights are obligations of a state to its citizens. Personal data protection is intended to guarantee citizens' rights to personal protection and raise public awareness and guarantee recognition and respect for the importance of personal data protection. However, in practice, many violations of the right to privacy occur. On October 17, 2022, Indonesia officially passed Law Number 27 of 2022 concerning Personal Data Protection (PDP Law). With the increasingly sophisticated development of information technology, the protection of personal data has become a vital issue for maintaining individual privacy rights and information security in cyberspace. Social facts related to violations of the right to freedom of personal data can be taken from incidents related to personal confidentiality experienced by customers of telecommunications service providers, banking, and online marketplaces. Therefore, it is very important to implement public understanding regarding personal data protection and legal sanctions for those who commit violations. Supervision and law enforcement must also be a concern for government institutions so that this law has the principles of certainty and benefit

Keywords: *Personal Data, Confidentiality and Legal Protection*

A. INTRODUCTION

Every citizen has constitutional rights, namely rights guaranteed by law. With these constitutional rights, the state has a constitutional obligation, namely to protect all citizens.

This constitutional obligation of the state is stated in the preamble to the 4th paragraph of the 1945 Constitution of the Republic of Indonesia (UUD RI 1945), which states that the state is obliged to protect all Indonesian people in improving general welfare, educating the nation's life, and implementing world order based on freedom, world peace, and social justice. (Danrivanto Budhijanto, 2023)

On October 17, 2022, Indonesia officially passed Law Number 27 of 2022 concerning Personal Data Protection (PDP Law). This law represents an important milestone in the country's efforts to protect its citizens' personal data in the rapidly evolving digital era. With the increasingly sophisticated development of information technology, the protection of personal data has become a vital issue for maintaining individual privacy rights and information security in cyberspace. (Teguh Prasetyo, Rizky PP Karo Karo, 2021)

Prior to the enactment of this Law, Indonesia did not have specific regulations that comprehensively regulate personal data protection. Although there are several related regulations, such as those stated in the ITE Law (Information and Electronic Transactions), namely Law of the Republic of Indonesia Number 11 of 2008 and updated by Law Number 1 of 2024 concerning Information and Electronic Transactions, the regulations are not sufficient to address the challenges and risks that arise from the widespread use of personal data in various sectors. (Latumahina, RE, 2014)

Violations of privacy frequently occur in Indonesia. For example, among the many social facts related to violations of the right to freedom of personal data, we can cite incidents related to privacy experienced by customers of telecommunications services, banking, and online marketplaces.(*Ibid*)

The term personal data is part of the right to privacy. The emergence of the term personal data is stated in Article 1 paragraph (1) of the Minister of Communication and Information Regulation Number 20 of 2016. In Article 1 paragraph (1) of the Regulation, "personal data" is defined as certain individual data that can be stored, maintained, and kept true and its confidentiality protected. Based on Article 1 paragraph (2) certain individual data is defined as any true and real information that is attached and can be identified, either directly or indirectly, to each individual whose use is in accordance with the provisions of laws and regulations. Then Article 1 paragraph (3) provides an explanation that the owner of personal data is the individual to whom certain individual data is attached. (Sinta Dwi Rosadi, 2023)

Personal data is a legal entity. If used for legal purposes, it creates obligations and rights

that must be fulfilled. If not, the aggrieved party can take legal action. The saying "what's in a name" is incorrect, as legally, a name is a personal data identity that must be protected from unauthorized use. Law Number 27 of 2022 aims to provide better protection for citizens' personal data. Some of the main objectives include:

a. Protecting citizens' privacy rights: Every individual has the right to control and protect their personal data, whether held by the government, companies, or other entities.

b. Preventing data misuse: This law strictly regulates how personal data can be collected, processed, used, and shared by third parties to prevent misuse that could harm individuals.

c. Ensuring personal data security: This law requires parties managing personal data to safeguard the security of that data from potential leaks or cyberattacks.

d. Increasing public trust: With clear and firm personal data protection, it is hoped that public trust in government administration and transactions in the digital world will be fostered. This is based on Article 26 of Ministerial Regulation of the Ministry of Communication and Information Technology Number 20 of 2016 concerning Personal Data Protection in Electronic Systems, which states that personal data owners have the right:

   1. Regarding the confidentiality of their personal data, they can file a complaint to the Minister regarding the resolution of personal data disputes regarding the failure of Electronic System Operators to protect the confidentiality of their personal data;

   2. Obtain access or the opportunity to change or update their personal data without disrupting the personal data management system, unless otherwise specified by statutory provisions;

   3. Obtain access or the opportunity to obtain historical personal data previously submitted to the Electronic System Provider, provided that it complies with statutory provisions; and

   4. Request the destruction of certain personal data belonging to them in the Electronic System managed by the Electronic System Provider, unless otherwise specified by statutory provisions. 6yt (Amboro, Florianus Yudhi Priyo, and Viona Puspita, 2025)

In this regard, it is considered very necessary to conduct outreach and research related to this matter, especially in the era of globalization and digitalization, therefore community service is carried out to socialize the understanding of personal data, the scope of personal data, its legal consequences, and penalties for those who commit violations. (*ibid*)

So, based on the explanation of the background that has been described above, the author is interested in raising the title LEGAL PROTECTION OF PERSONAL DATA CONFIDENTIALITY IN THE DIGITALIZATION ERA REVIEWED FROM LAW NUMBER 27 OF 2022 CONCERNING PERSONAL DATA PROTECTION

B. FOCUS AND PROBLEM

Based on the background of the problems described above, the authors formulate the problem as follows : What is the form of Legal Protection For Personal Data Confidentiality In The Digitalization Era and What are the challenges faced in implementing the protection of personal data confidentiality in the digital era based on the Personal Data Protection Law?

C. MATERIALS AND METHODS

The type of research used is normative legal research which is a legal research conducted by examining library materials or primary or secondary materials. Empirical legal research is also conducted, which is a type of research used to look at legal aspects in social interactions in society, in order to truly understand the dasollen and dasein between applicable legal rules and the public's understanding regarding this law as well as its supervision and implementation. So it is hoped that legal rules are not only on paper, but can be realized as certainty, benefit and justice. (Kusnadi, Sekaring Ayumeida, 2021)

In this study, a method will be used through material presentation and interactive discussions between the speaker and the audience to determine the depth of understanding of the material presented before the presentation and after the presentation, because the target audience is expected to be able to understand the meaning of personal data, the scope of personal data, efforts made to maintain the confidentiality of personal data, legal protection provided by the state and sanctions imposed on parties who violate Law Number 27 of 2022 concerning Personal Data Protection (PDP Law).

The legal materials used are primary legal materials. Primary legal materials are authoritative, meaning they possess authority. They are legally binding. Primary materials consist of legislation, ministerial regulations, and other legal provisions. This compilation focuses on Law Number 27 of 2022 concerning Personal Data Protection and Law of the Republic of Indonesia Number 11 of 2008, as amended by Law Number 1 of 2024 concerning Electronic Information and Transactions.

In addition to primary legal materials, this study also utilizes secondary legal materials,

which provide explanations of primary legal materials. Secondary legal materials consist of all publications that are not official documents. These publications include textbooks, legal dictionaries, legal journals, court decisions, and related scientific works. The author also considers tertiary sources, namely materials that provide guidance or explanations of primary and secondary legal materials, such as legal dictionaries, encyclopedias, newspapers, and others.

Then, conclusions are drawn that are useful for answering the problem formulation and objectives of this research. The results of the analysis are presented descriptively, namely by describing the actual situation in the field, resulting in a descriptive-qualitative description of the research results, which will then provide meaning and conclusions to answer the problem.

D. RESULT AND DISCUSSION

1. THE FORM of LEGAL PROTECTION PROVIDED by THE PDP LAW AGAINST VIOLATIONS OF PERSONAL DATA CONFIDENTIALITY, INCLUDING LAW ENFORCEMENT MECHANISMS AND SANCTIONS

In Law No. 27 of 2022 concerning Personal Data Protection (PDP Law), data subjects, namely individuals whose data is collected and processed, are granted various rights to protect their personal information. These rights aim to give everyone full control over their data, while ensuring that the data is used transparently and responsibly by data controllers. Data subjects have the right to know clearly how their personal data is collected, used, stored, and shared. They also have the right to give or withdraw consent to data processing and can request the deletion of data that is no longer relevant or collected illegally. In addition, data subjects can file objections if their data is processed for purposes inconsistent with their initial consent, and can even request the restriction of data processing to only certain purposes.(M.H. Zaid, 2024)

The complexity of understanding and implementing the principle of the right to privacy regarding personal data in the digital era, as well as the challenges in implementing regulations that recognize personal data as an individual's privacy right. In an increasingly connected digital era dominated by information technology, the principle of the right to privacy regarding personal data has become increasingly important, but also increasingly complex. The use of technologies such as the internet, social media, and smart devices has enabled the massive collection, storage, and processing of personal data. (Dhoni, Dr Dhoni Martien, 2023)

The main challenge that arises is how to ensure that individuals' privacy rights are respected and protected in this increasingly complex context. Furthermore, although regulations

governing personal data protection as a privacy right exist, their implementation still faces various obstacles. These include a lack of public awareness of their privacy rights, weak law enforcement against data privacy violations, and imperfections in existing regulations and policies. (Ridho Sa'dillah Ahmad, et al, 2025)

Implementation of the PDP Law requires significant investment, especially for sectors that manage large amounts of data, such as banking, hospitals, and technology companies. Companies must develop cybersecurity infrastructure, update systems, and train employees to be able to comply with new standards. (Rosadi, Sinta Dewi., 2015)

The Personal Data Protection Law provides two main forms of legal protection:

A. Preventive Protection

This protection aims to prevent breaches of personal data confidentiality. This includes: Obligations of Data Controllers to Ensure Data Security. Controllers are required to provide adequate security systems (encryption, limited access, audits), ensure data confidentiality, integrity, and availability, and avoid excessive data collection (data minimization).

Processing personal data must be based on the explicit consent of the data subject, except in certain circumstances stipulated by law.

The Personal Data Protection Law regulates various rights, such as: the right to information, the right to access, the right to rectify data, the right to erase data, the right to withdraw consent, and the right to object to processing. These rights prevent data misuse from the outset.

Certain data controllers/processors are required to appoint a data protection officer, particularly for public institutions, large-scale controllers, and high-risk data processors.

If a data breach occurs, the controller is required to notify the data subject within 3 x 24 hours, including the cause, impact, and remedial measures. This ensures that victims can take immediate security measures.

B. Repressive Protection (Enforcement)

This protection applies when a violation has occurred.

Dispute Resolution Mechanism The Personal Data Protection Law provides several avenues for resolution:

1. Complaints to the Data Supervisory Authority

   Data subjects have the right to report data leaks, misuse of data, or denial of rights by the controller. The authority can conduct investigations and impose administrative sanctions.

   Administrative sanctions (reprimands, fines, processing suspensions) and criminal sanctions

(imprisonment and large fines) are possible.

2. Out-of-Court Dispute Resolution Through Mediation, Arbitration, and Alternative Dispute Resolution (APS).
3. Civil Lawsuits in Court (litigation)

   Data subjects can claim material damages and immaterial damages if they are proven to have suffered losses due to a data confidentiality breach.

2. CHALLENGES IN IMPLEMENTING THE PERSONAL DATA PROTECTION LAW

Challenges in the implementation of the Personal Data Protection Law include:

1. The suboptimal formation and readiness of a data supervisory authority (Data Protection Authority). The Personal Data Protection Law mandates the existence of a supervisory body responsible for monitoring, auditing, and enforcing sanctions. However, challenges arise because the institutional structure is not yet fully established, the availability of expert human resources in digital forensics, cybersecurity, and technology law is still limited, and cross-agency coordination mechanisms are suboptimal.
2. Low Public Privacy Awareness and Literacy: Many people do not understand their rights as data subjects, often provide personal data without reading the terms and conditions, and are unaware of complaint procedures in the event of a violation. This low literacy makes enforcing data subjects' rights ineffective.
3. Unequal Compliance of Data Controllers and Processors. Many companies, especially MSMEs and startups, face challenges, as evidenced by a lack of understanding of legal obligations (DPIA, retention policies, breach notifications), limited budgets for system security, and inadequate ICT infrastructure. Consequently, compliance levels vary between large and small companies.
4. Increasingly complex cybersecurity threats in the digital era are characterized by increasingly sophisticated cyberattacks (phishing, ransomware, data scraping, AI-driven attacks), repeated data leaks involving sensitive data (NIK, biometrics, health), and weak security standards in several public and private service systems. This increases the risk of data confidentiality breaches.
5. Lack of Transparent Accountability Mechanisms. Although the PDP Law stipulates mandatory notification of data breaches, in reality, not all data controllers provide prompt notification. Victims often lack clarity regarding the cause and impact, and the

investigation process often takes a long time. This weakens the accountability of data controllers.

6. Challenges of Cross-Border Data Transfer. Many digital services use servers and cloud services located overseas. Consequently, many problems arise, including differences in data protection standards between countries, difficulties in ensuring compliance with the PDP Law by foreign parties, the potential for illegal access by foreign parties, and the need for strict oversight mechanisms for cross-border data transfer.
7. Technological Development Outpaces Regulation. The emergence of innovations such as Artificial Intelligence (AI), Big Data Analytics, the Internet of Things (IoT), Biometrics, and Blockchain creates new privacy challenges that are not yet fully regulated in the PDP Law.
8. Weak Administrative Culture in Data Management. Public and private agencies often face challenges such as substandard archive and data management, excessive data collection, and a lack of routine security audits. This increases the risk of leakage.

E. CONCLUSION

1. Sensitive personal data is an integral part of a person's life. Information such as name, address, identity number, medical data, and financial information are examples of highly sensitive personal data and can have significant impacts on individuals if misused. Therefore, personal data protection is not only important from a security perspective but also as part of an individual's right to privacy. The right to privacy includes individuals' control over their personal information and the ability to protect themselves from misuse of that data. Law Number 27 of 2022 concerning Personal Data Protection is a significant step forward in strengthening personal data protection in Indonesia. Despite facing challenges such as low digital literacy, high implementation costs, and unclear oversight structures, this law and public awareness.(Suari, Kadek Rima Anggen, and I. Made Sarjana, 2023)
2. The successful implementation of the PDP Law depends on several important factors, namely, massive public education, strengthening the capacity of companies and government agencies to manage data, and consistent and fair law enforcement. If these steps are carried out optimally, Indonesia can build a data protection system while protecting the privacy rights of citizens in the digital era. (Rudi Natamiharja, Rudi Natamiharja, and Mindoria Stefany, 2019)

REFERENCES

A. Buku dan Jurnal

Amboro, Florianus Yudhi Priyo, and Viona Puspita. "Perlindungan Hukum Atas Data Pribadi (Studi Perbandingan Hukum Indonesia dan Norwegia)." *CoMBInES-Conference on Management, Business, Innovation, Education and Social Sciences*. Vol. 1. No. 1. 2021.

Budhijanto, Danrivanto. "Hukum Pelindungan Data Pribadi Di Indonesia Cyberlaw & Cybersecurity." *Bandung: Refika Aditama* (2023)

Dhoni, Dr Dhoni Martien. "Perlindungan Hukum Data Pribadi." (2023).

Enterprise, Jubilee. *Trik Mengamankan Password*. Elex Media Komputindo, 2013.

M. H. Zaid, " Perlindungan Privasi dan Data Pribadi", PT Intrans Publishing, Jakarta, 2024.

Kusnadi, Sekaring Ayumeida. "Perlindungan hukum data pribadi sebagai hak privasi." *AL WASATH Jurnal Ilmu Hukum* 2.1 (2021): 9-16.

Latumahina, Rosalinda Elsina. "Aspek Hukum Perlindungan Data Pribadi di Dunia Maya." (2014).

Rosadi, Sinta Dewi. *Cyber law: aspek data privasi menurut hukum internasional, regional, dan nasional*. Refika Aditama, 2015.

Rudi Natamiharja, Rudi Natamiharja, and Mindoria Stefany. "Perlindungan Hukum Atas Data Pribadi Di Indonesia (Studi Terhadap Pelaksanaan Pelayanan Jasa Telekomunikasi Pt. Telekomunikasi Selular)." *Prodigy Jurnal Perundang undangan* 7.2 (2019).

Simanjuntak, Predderics Hockop. "Perlindungan Hukum Terhadap Data Pribadi pada Era Digital di Indonesia: Studi Undang-Undang Perlindungan Data Pribadi dan General Data Protection Regulation (GDPR)." *Jurnal Esensi Hukum* 6.2 (2024): 105-124.

Sinta Dwi Rosadi," Pembahasan Tentang UU Data Perlindungan Data Pribadi, PT Sinar Grafika, Jakarta, 2023.

Suari, Kadek Rima Anggen, and I. Made Sarjana. "Menjaga privasi di era digital: Perlindungan data pribadi di Indonesia." *Jurnal Analisis Hukum* 6.1 (2023): 132-142.

Teguh Prasetyo, Rizky PP Karo Karo" Pengaturan Perlindungan Data Pribadi di Indonesia", PT Nusa Media, Bandung, 2021.

B. Internet

https://fh.untar.ac.id/2025/09/11/perlindungan-data-pribadi-implementasi-uu-no-27-tahun-2022, diakses pada tanggal, 04 Desember 2025.

C. Perundang –Undangan :

Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi.

Undang-Undang Republik Indonesia Nomor 1 Tahun 2024 Tentang Informasi dan Transaksi Elektronik.

Peraturan Kementrian Kominfo Nomor 20 Tahun 2016 Tentang Perlindungan Data Pribadi Dalam Sistem Elektronik.