



Safeguarding Individual Rights Amid Personal Data Security Breaches

Relly Vivianda^{1*} & Khalisah Hayatuddin²

^{1,2}Universitas Muhammadiyah
Palembang, Indonesia

Correspondence

Relly Vivianda, Universitas
Muhammadiyah Palembang,
Indonesia, Jl. Jenderal Ahmad Yani
Kampus A, 13 Ulu, Kec. Seberang
Ulu II, Kota Palembang, Sumatera
Selatan 30263, e-mail:
viviandarelly@gmail.com

How to cite

Vivianda, Relly., & Hayatuddin,
Khalisah. 2027. Safeguarding
Individual Rights Amid Personal
Data Security Breaches. *Jurnal Ilmu
Hukum Kyadiren* 8(2), 111-124.
<https://doi.org/10.46924/jihk.v8i2.532>

Original Article

Abstract

Digital transformation has increased reliance on the collection and processing of personal data while simultaneously intensifying the risks of data breaches, misuse, and unauthorized access. These threats may undermine individuals' fundamental rights to privacy and data security. This study aims to analyze the legal status of personal data security and confidentiality as individual and constitutional rights and to examine the extent to which personal data protection mechanisms are aligned with Law Number 27 of 2022 on Personal Data Protection (the PDP Law). Employing a normative legal research method and statutory and conceptual approaches, this study analyzes relevant legislation, legal doctrines, and scholarly literature. The findings indicate that the security and confidentiality of personal data constitute integral elements of personal protection and are grounded in constitutional rights. The PDP Law establishes a comprehensive regulatory framework governing personal data processing, data subject rights, the obligations of data controllers and processors, security measures, and accountability. Nevertheless, the effectiveness of legal protection remains contingent on consistent implementation, effective regulatory oversight, adequate digital literacy, and robust law enforcement.

Keywords: *Data Protection, Individual Rights, Privacy, Digital Transformation*

Abstrak

Perkembangan digital meningkatkan ketergantungan pada pengumpulan dan pemrosesan data pribadi, sekaligus memperbesar risiko kebocoran, penyalahgunaan, dan akses tanpa hak yang dapat mengancam hak individual atas privasi dan keamanan. Penelitian ini bertujuan menganalisis kedudukan hak atas keamanan dan kerahasiaan data pribadi sebagai bagian dari hak individual dan hak konstitusional serta mengkaji kesesuaian mekanisme perlindungan data pribadi dengan Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi. Penelitian ini menggunakan metode yuridis normatif dengan pendekatan perundang-undangan dan konseptual melalui analisis terhadap peraturan perundang-undangan, doktrin hukum, dan literatur ilmiah yang relevan. Keamanan dan kerahasiaan data pribadi merupakan bagian integral dari perlindungan diri pribadi yang berlandaskan hak konstitusional. UU PDP telah menyediakan kerangka komprehensif mengenai pemrosesan, hak subjek data, kewajiban pengendali dan prosesor, keamanan, serta pertanggungjawaban. Namun, efektivitas perlindungan masih bergantung pada konsistensi implementasi, pengawasan, literasi digital, dan penegakan hukum.

Kata kunci: *Pelindungan Data, Hak Individual, Privasi, Perkembangan Digital*

1. INTRODUCTION

As a rule-of-law state, Indonesia establishes law as the foundation for the exercise of state power and as an instrument for safeguarding the rights of every individual. Accordingly, actions undertaken by the government, state institutions, and other entities whose activities affect the public must comply with the law while upholding justice, legal certainty, and human rights. The protection afforded to individuals extends beyond physical security, freedom, and protection from discrimination to include the protection of personal life and privacy. Article 28G(1) of the 1945 Constitution of the Republic of Indonesia provides a constitutional basis for protecting an individual's person, family, honor, dignity, and property. The Constitutional Court has further affirmed that personal data protection constitutes an integral component of the constitutional right to personal protection.

Digital transformation has enabled data to be collected, stored, processed, exchanged, and integrated rapidly across various sectors, including commerce, finance, health care, education, and public services.¹ Although these developments provide significant convenience and efficiency, they have also increased public reliance on electronic systems and expanded the risks of unauthorized access, use, disclosure, and processing of personal data.² Consequently, data breaches, identity theft, misuse of information, and the processing of personal data without consent can no longer be viewed solely as technical cybersecurity concerns. Rather, they have become significant legal issues because they may infringe upon privacy rights and cause material and non-material harm to data subjects.

The urgency of personal data protection is evident in various data breach incidents involving digital platforms in Indonesia, including Tokopedia, Bukalapak, and TokoTalk.³ These incidents demonstrate a growing disparity between the rapid adoption of digital technologies and the need to ensure the security and confidentiality of personal data. Therefore, the state cannot merely develop a digital ecosystem; it must also establish and ensure the effective implementation of legal safeguards. The enactment of Law No. 27 of 2022 on Personal Data Protection (the PDP Law) represents a significant milestone in this regard, as it establishes a more comprehensive

¹ Margaretha Hanita, "Transformasi Ketahanan Wilayah Pada Era Digital: Peran Kepemimpinan Digital Dalam Membangun Smart City Di Kota Pariaman Sumatera Barat," *Jurnal Ketahanan Nasional* 29, no. 2 (2023): 178–98, <https://doi.org/10.22146/jkn.86067>.

² Alifah Jasmine Kallista Remanu et al., "Analisis Transformasi Digital Pelayanan Publik Identitas Kependudukan Digital (IKD) Dalam Implementasi Digital Governance Di Suku Dinas Kependudukan Dan Pencatatan Sipil Jakarta Selatan," *Jurnal Kolaboratif Sains* 9, no. 5 (2026): 3691–707, <https://doi.org/10.56338/jks.v9i5.10899>.

³ Sinta Anastasya, "Kebocoran Data 15 Juta Pengguna E-Commerce: Ancaman Nyata Keamanan Digital Di Indonesia," *Kompasiana*, Kompasiana, 2026, https://www.kompasiana.com/sintaanastasya0349/695cb04aed6415211e61ad44/kebocoran-data-15-juta-pengguna-e-commerce-ancaman-nyata-keamanan-digital-di-indonesia#goog_rewarded.

legal framework governing data subject rights, personal data processing, the obligations of data controllers and processors, and sanctions for violations.

Research on personal data protection in Indonesia has developed alongside the expanding use of digital technologies, although individual studies have emphasized different dimensions of the issue. Agusta, for example, examines the protection of borrowers' personal data in peer-to-peer lending services. The study demonstrates that financial technology innovations have expanded public access to financial services while simultaneously increasing the risk of personal data misuse. Its primary focus is on the protection of borrowers' data within the broader relationship between financial technology and economic activity.⁴

Purnama and Alhakim broaden this discussion by highlighting the absence, at the time of their study, of specific and comprehensive legislation governing personal data protection. They argue that the applicable regulatory framework remained fragmented across various legislative instruments, creating a need for dedicated legislation capable of providing greater legal certainty.⁵ These findings are consistent with those of Suharyanti and Sutrisni, who argue that the rapid growth of online media has not been accompanied by adequate preventive legal protection. They further demonstrate that personal data breaches may give rise to civil, administrative, and criminal legal consequences.⁶

Buana examines the misuse of personal data in peer-to-peer lending services and concludes that sector-specific regulations have not provided optimal or comprehensive protection. The study proposes strengthening data protection systems and promoting interinstitutional cooperation as potential solutions.⁷ Meanwhile, Saputra, Kurnia, Rahmah, and Sumarni broaden the analytical perspective by connecting privacy, digital ethics, data security, big data, and social media with the need for regulatory harmonization within the digital economy.⁸

Subsequent regulatory developments have shifted the focus of research toward the implementation and effectiveness of the PDP Law. Utami argues that Law No. 27 of 2022 provides greater normative clarity and strengthens the legal framework for

⁴ Hendrawan Agusta, "Perlindungan Data Pribadi Penerima Pinjaman dalam Transaksi Pinjam Meminjam Uang Berbasis Teknologi Informasi: Peer To Peer Lending," *Jurnal Hukum & Pembangunan* 50, no. 4 (2020): 780–809, <https://doi.org/10.21143/jhp.vol50.no4.1029>.

⁵ Thiara Dewi Purnama and Abdurrahman Alhakim, "Pentingnya UU Perlindungan Data Pribadi Sebagai Bentuk Perlindungan Hukum Terhadap Privasi Di Indonesia," *Jurnal Komunitas Yustisia* 4, no. 3 (2021): 1056–64, <https://doi.org/10.23887/jatayu.v4i3.44370>.

⁶ Ni Putu Noni Suharyanti and Ni Komang Sutrisni, "Urgensi Perlindungan Data Pribadi Dalam Menjamin Hak Privasi Masyarakat," *Prosiding Seminar Nasional Fakultas Hukum Universitas Mahasaraswati Denpasar* (Denpasar) 1, no. 1 (2020): 119–34, <https://e-journal.unmas.ac.id/index.php/psnfh/article/view/2395>.

⁷ Sandy Ekki Wiratama Buana, "Perlindungan Hukum Terhadap Data Pribadi Kepada Pemilik Data Pribadi Dalam Penyelenggaraan Jasa Fintech Peer To Peer Lending" (Universitas Islam Indonesia, 2022), <https://dspace.uui.ac.id/handle/123456789/39314>.

⁸ Beni Andrian Saputra et al., "Penerapan Privasi Dan Etika Di Era Digital Dalam Perlindungan Data Pribadi," *Musytari: Neraca Manajemen, Akuntansi, Dan Ekonomi* 5, no. 9 (2024), <https://ejournal.warunayama.org/index.php/musytarineraca/article/view/3570/3351>.

addressing violations of personal data protection.⁹ Similarly, Fachri, Khaerudin, and Dewi and Tanuwidjaja demonstrate that the PDP Law has established a more comprehensive legal foundation, although its implementation continues to face challenges related to public awareness, system security, regulatory oversight, and law enforcement.¹⁰ Using a socio-legal approach, Amalia, Yoga, and Maharani further identify a gap between legal norms and their implementation in practice, particularly as a result of limited institutional capacity, low levels of public digital literacy, and suboptimal integration of technology into data protection mechanisms.¹¹

Previous research reveals a limited number of studies that systematically connect individual rights as constitutional rights with data protection obligations, legal accountability mechanisms, and the effectiveness of law enforcement in addressing digital data security breaches. This study therefore approaches data security breaches not merely as technical or regulatory problems, but as violations of individual rights that require an integrated legal response encompassing preventive, repressive, and remedial measures.

Against this backdrop, this study aims to analyze the legal protection of individual rights in cases of personal data security breaches within digital systems in Indonesia. The analysis focuses on two main issues: (1) the legal status of the right to personal data security and confidentiality as a component of individual and constitutional rights; and (2) the extent to which personal data protection mechanisms comply with the provisions of Law No. 27 of 2022 on Personal Data Protection.

2. RESEARCH METHODOLOGY

This study employs a normative legal research method using statutory, conceptual, and case approaches. The research focuses on analyzing the legal protection of individual rights in the context of breaches of personal data security and confidentiality in Indonesia. The statutory approach is used to examine the 1945 Constitution of the Republic of Indonesia, Law No. 27 of 2022 on Personal Data Protection (the PDP Law), and other regulations governing electronic systems, electronic information and transactions, and human rights. The conceptual approach is employed to examine key legal concepts, including the rule of law, legal protection, individual rights, privacy, data security, confidentiality, and legal liability. The case approach is used to assess the

⁹ Sal Sabila Khoirotunnisa Utami, "Personal Data Protection and Its Regulatory Frameworks Under Cyber Law," *Domus Legalis Cogitatio* 1, no. 2 (2024): 175–93, <https://doi.org/10.24002/dlc.v1i2.9894>.

¹⁰ Faisal Fachri et al., "Protection of Digital Privacy Rights as a Human Right Against Personal Data Misuse in Indonesia," *Journal of International Islamic Law, Human Right and Public Policy* 4, no. 3 (2026): 1332–37, <https://doi.org/10.5281/ZENODO.21853686>; Carissa Tanuwidjaja, "Protection of Personal Data in the Digital Era: Legal Analysis and Implementation Challenges in Indonesia," *Journal of Legal Studies Judex Praetor* 2, no. 1 (2026): 1–19, <https://doi.org/10.35671/judex.v2i1.174>.

¹¹ Rina Amalia et al., "Legal Protection of Personal Data in the Digital Era: Challenges and Regulatory Framework in Indonesia," *Journal of Lex et Justitia* 2, no. 1 (2026): 50–65, <https://doi.org/10.67171/mnrwww36>.

relationship between *das sollen* (the normative legal ideal) and *das sein* (the law as implemented in practice), particularly in cases involving personal data breaches and misuse.

The legal materials consist of primary, secondary, and tertiary sources selected purposively based on their relevance to the research questions. Data were collected through a comprehensive literature review involving the examination of legislation, court decisions, books, and scholarly articles. The materials were analyzed using qualitative descriptive and prescriptive methods through several stages, including legal inventory, classification, interpretation, normative harmonization, and case analysis. Normative triangulation was employed to ensure the consistency and validity of the legal arguments and to formulate recommendations for strengthening personal data protection, legal accountability, law enforcement, and effective remedies for data subjects whose rights have been violated.

3. RESEARCH RESULT AND DISCUSSION

3.1. Position of the Right to Personal Data Security and Confidentiality as an Individual and Constitutional Right

The security and confidentiality of personal data cannot be treated solely as technical matters of information security. Rather, they constitute substantive elements of individual rights protection that derive constitutional legitimacy from guarantees of personal protection, honor, dignity, and security under the 1945 Constitution of the Republic of Indonesia. The position of the right to personal data security and confidentiality can be understood through three interrelated dimensions: individual rights, privacy rights, and constitutional rights.

At the individual level, personal data represents an individual's identity and various aspects of personal life that are intrinsically connected to the data subject.¹² Accordingly, individuals have a legitimate legal interest in determining how information concerning them is collected and used, to whom it may be disclosed, and for what purposes it may be processed. Breaches of data security and confidentiality may result not only in economic or administrative losses but also in interference with individual autonomy, personal security, reputation, and control over information concerning oneself.¹³

At the constitutional level, this position is particularly significant because Article 28G(1) of the 1945 Constitution guarantees the protection of the person, family, honor, dignity, and sense of security of every individual. The right to personal data security is closely connected to these constitutional guarantees because the use or disclosure of

¹² Siti Mardiyati, "Konstitusionalitas Perlindungan Data Pribadi Sebagai Bagian Dari Hak Atas Rasa Aman," *Consensus: Jurnal Ilmu Hukum* 4, no. 2 (2025): 221–33, <https://doi.org/10.46839/consensus.v4i2.1758>.

¹³ Putri Regina S. Pakaya et al., "Dampak Penyebaran Data Pribadi Melalui Media Digital Terhadap Perlindungan Hak Privasi," *Jurnal Hukum Bisnis* 15, no. 1 (2026): 17–26, <https://doi.org/10.47709/jhb.v15i01.7594>.

personal data without a valid legal basis may intrude upon an individual's private sphere and undermine personal security. This relationship demonstrates that personal data protection is not merely an administrative or regulatory matter but also constitutes part of the state's constitutional obligation to respect and protect citizens' fundamental rights. In this context, Constitutional Court Decision No. 151/PUU-XXII/2024 further reinforces this legal construction by emphasizing the relationship between personal data protection and the right to personal protection guaranteed under Article 28G(1) of the 1945 Constitution.

The legal construction of personal data protection in Indonesia has also undergone significant development following the enactment of Law No. 27 of 2022 on Personal Data Protection (the PDP Law). Before the PDP Law entered into force, provisions governing personal data were dispersed across various sectoral regulations, including those concerning population administration, health, communications, and electronic transactions. Although these regulations provided protection for particular aspects of personal data, they did not constitute an integrated and comprehensive legal framework. The PDP Law subsequently established a more systematic framework governing the categories of personal data, data subject rights, lawful bases for processing, the obligations of data controllers and processors, cross-border data transfers, administrative sanctions, prohibited conduct, and criminal provisions. This framework has transformed the legal position of personal data from merely an administrative object or information possessing economic value into an object of legal protection directly associated with individual rights.

The right to personal data security and confidentiality derives further significance from the obligation of entities engaged in data processing to ensure that processing activities are conducted lawfully, limited to legitimate purposes, and accompanied by adequate safeguards. Confidentiality requires personal data to be accessible or used only by authorized parties for legitimate purposes, whereas security requires the implementation of measures designed to prevent loss, misuse, unauthorized access, alteration, disclosure, and other forms of violation.¹⁴ Accordingly, security and confidentiality constitute two inseparable dimensions of personal data protection. Security without confidentiality cannot ensure appropriate restrictions on access, while confidentiality without adequate security mechanisms cannot effectively prevent data breaches.

Agusta emphasizes the importance of protecting borrowers' personal data in financial technology (fintech) transactions to prevent misuse and the resulting legal consequences. Purnama and Alhakim similarly underscore the need for specific legislation because the regulatory framework preceding the PDP Law remained

¹⁴ Sylvia Faradina Amandasari Arthaputri, "Perlindungan Data Pribadi Sebagai Bentuk Perwujudan Cyber Security: Studi Komparatif Indonesia Dan Singapura," *Dinamika: Jurnal Ilmiah Hukum* 30, no. 1 (2024).

fragmented across various legal instruments.¹⁵ Meanwhile, Suharyanti and Sutrisni demonstrate that violations of privacy and personal data may give rise to civil, administrative, and criminal liability, while preventive legal protection remains suboptimal.¹⁶ Buana focuses more specifically on personal data misuse in fintech services and proposes strengthening consumer protection systems and data security mechanisms.¹⁷ Saputra et al. further broaden the discussion by connecting personal data protection with ethical and moral considerations in the digital environment.¹⁸

Issues concerning personal data extend beyond whether an organization has fulfilled its administrative obligations; they also concern whether the state and data controllers respect individuals' fundamental rights to security and control over their personal information. This perspective is particularly relevant in the context of digitalization, which enables personal data to be collected and processed on a massive scale and exchanged across institutions and jurisdictions.

Developments in international law, including principles reflected in the General Data Protection Regulation (GDPR), provide an important reference point for strengthening Indonesia's personal data protection framework. Although the GDPR is not directly binding on Indonesia, principles such as lawfulness, fairness, transparency, purpose limitation, data minimization, accuracy, storage limitation, integrity, and confidentiality reflect evolving international standards that place individual rights at the center of personal data processing. These principles may serve as relevant references for legal interpretation and policy development, but their application must remain consistent with Indonesia's national legal framework and the distinctive characteristics of its legal system.

Personal data breaches and misuse must therefore be understood as violations of rights rather than merely technological failures. Although digital security systems constitute essential instruments of protection, effective personal data protection requires an integrated framework encompassing technical safeguards, legal compliance, data governance, transparency, regulatory oversight, and accountability mechanisms. When personal data is accessed by unauthorized parties, processed for purposes beyond legitimate objectives, or disclosed without a valid legal basis, the consequences extend beyond the compromise of database security. Such conduct may infringe upon individuals' rights to privacy, security, dignity, and control over information concerning themselves.

The right to personal data security and confidentiality constitutes an integral component of individual rights that receive constitutional protection. The Personal Data

¹⁵ Purnama and Alhakim, "Pentingnya UU Perlindungan Data Pribadi Sebagai Bentuk Perlindungan Hukum Terhadap Privasi Di Indonesia."

¹⁶ Suharyanti and Sutrisni, "Urgensi Perlindungan Data Pribadi Dalam Menjamin Hak Privasi Masyarakat."

¹⁷ Buana, "Perlindungan Hukum Terhadap Data Pribadi Kepada Pemilik Data Pribadi Dalam Penyelenggaraan Jasa Fintech Peer To Peer Lending."

¹⁸ Saputra et al., "Penerapan Privasi Dan Etika Di Era Digital Dalam Perlindungan Data Pribadi."

Protection (PDP) Law serves as the primary legal instrument for operationalizing this protection by translating constitutional and individual rights into concrete obligations for data controllers and processors and establishing accountability mechanisms for violations. Nevertheless, the mere existence of legal norms does not, by itself, ensure effective protection. The effectiveness of personal data protection depends on consistent law enforcement, adequate supervisory capacity, public awareness of data subjects' rights, compliance by data controllers, robust security systems, and accessible and effective remedies.

Accordingly, the protection of personal data security and confidentiality should be grounded in a rights-based approach. Such an approach requires every policy, regulatory measure, and data processing activity to be directed not merely toward maintaining system security but, more fundamentally, toward respecting, protecting, and fulfilling the constitutional rights of every individual.

3.2. Alignment of Personal Data Protection Mechanisms with Law No. 27 of 2022 on Personal Data Protection

Substantively, Law No. 27 of 2022 on Personal Data Protection (the PDP Law) establishes a relatively comprehensive legal framework governing the lifecycle of personal data processing. This framework encompasses personal data protection principles, data classification, data subject rights, lawful bases for processing, the obligations of data controllers and processors, data transfers, administrative sanctions, prohibited conduct, and criminal provisions. Accordingly, data protection mechanisms are no longer concerned solely with the physical or technical security of databases but also with the lawfulness of every data processing activity. Compliance with the PDP Law must therefore be assessed across the entire data lifecycle, from collection and use to storage, disclosure, transfer, and deletion.

A key indicator of compliance is the existence of a lawful basis for processing personal data. The PDP Law requires data controllers to establish a processing basis consistent with applicable legal requirements, including valid and explicit consent, the performance of a contract, compliance with a legal obligation, the protection of vital interests, the performance of a task carried out in the public interest or in the exercise of official authority, and other legitimate grounds recognized by law. An organization's possession or control of personal data does not automatically confer authority to use that data for any purpose. This principle is essential for limiting potential misuse because personal data processing must have a legitimate and accountable purpose and must remain within the scope authorized by law.

Protection mechanisms that comply with the PDP Law must also effectively enable data subjects to exercise their legally recognized rights. Data subjects have various rights, including the right to obtain information concerning the processing of

their personal data, access their personal data, correct inaccurate data, and request the deletion or destruction of personal data under circumstances specified by law, as well as other rights provided under the PDP Law. These rights reflect a paradigm shift from a protection model centered primarily on institutional obligations toward a rights-based model that gives individuals greater control over their personal data. A protection mechanism should therefore not be considered adequate merely because an organization has established data security policies. It must also ensure that individuals have meaningful and effective means to understand how their data are processed, access their data, request corrections, and, where legally permissible, request their deletion or destruction.

The obligations of data controllers and processors constitute another central component of the PDP Law. It is insufficient for a data controller merely to provide a system for storing personal data; it must also ensure that all processing activities are conducted in accordance with applicable legal requirements, with due regard for data security and the prevention of unauthorized processing.¹⁹ Similarly, a data processor cannot be regarded as entirely free from legal responsibility merely because it processes personal data on the basis of instructions and predetermined purposes established by the controller.²⁰ When a processor performs processing activities beyond the scope of the controller's instructions or authorized purposes, legal liability may arise under the PDP Law. Personal data protection is therefore an institutional responsibility that extends throughout the entire processing chain rather than a purely technical responsibility assigned to system administrators.

An effective data protection mechanism must integrate preventive safeguards, incident response, and recovery measures designed to protect data subjects. Preventive safeguards include access controls, information system security, internal governance, purpose limitations, and measures to enhance personnel awareness and competence.²¹ When a protection failure or personal data breach occurs, the response mechanism must enable the organization to promptly identify, contain, manage, and report the incident in accordance with applicable legal obligations. Following an incident, protection efforts should not be limited to restoring or strengthening system security. They must also address the rights and interests of affected data subjects and the potential legal

¹⁹ Jonathan Matthew Pakpahan, "Kesadaran Urgensi Peran Pengendali Dan Prosesor Data Pribadi Dalam Rangka Pelindungan Data Pribadi Individu Berdasarkan Undang-Undang Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi," *Jurnal Hukum To-Ra : Hukum Untuk Mengatur Dan Melindungi Masyarakat* 10, no. 1 (2024): 119–37, <https://doi.org/10.55809/tora.v10i1.331>.

²⁰ Reginaldus Arfan Jebaru and Men Wih Widiatno, "Perlindungan Hukum Bagi Prosesor Data Pribadi Dalam Melaksanakan Pemrosesan Data Pribadi Menggunakan Aplikasi Sistem Informasi Kependudukan: Penelitian," *Jurnal Pengabdian Masyarakat Dan Riset Pendidikan* 4, no. 3 (2026): 19564–72, <https://doi.org/10.31004/jerkin.v4i3.5184>.

²¹ Mario Alvember and Dyah Permata Budi Asri, "Analisis Keamanan Data Pribadi Konsumen Terhadap Regulasi Pencantuman Nomor Induk Kependudukan Untuk Registrasi Nomor Telepon," *Arus Jurnal Sosial Dan Humaniora* 5, no. 2 (2025): 3017–26, <https://doi.org/10.57250/ajsh.v5i2.1590>.

consequences arising from the breach. The adequacy of a personal data protection mechanism should therefore not be measured solely by the existence or sophistication of security technologies but by the effectiveness of the overall governance framework operating before, during, and after a data security incident.²²

Agusta emphasizes that personal data protection in technology-based transactions requires mechanisms capable of preventing unauthorized parties from misusing personal data.²³ Purnama and Alhakim highlight the importance of specific legislation, noting that the regulatory framework preceding the PDP Law was fragmented across various sectoral regulations.²⁴ Suharyanti and Sutrisni observe that personal data breaches may give rise to various forms of legal liability and that preventive protection under the previous regulatory framework remained suboptimal.²⁵ Buana further argues that personal data protection in the fintech sector requires stronger institutional arrangements and more robust security systems.²⁶ Meanwhile, Saputra et al. broaden the discussion by incorporating ethical considerations and public awareness concerning the use of personal data in digital environments.²⁷

This study extends previous research by systematically examining the alignment of personal data protection mechanisms with the liability framework established under the PDP Law. The analysis, however, focuses not merely on the existence of regulations but also on whether the essential components of personal data protection—including lawful processing grounds, data subject rights, the obligations of data controllers and processors, security, confidentiality, oversight, accountability, and remedies—have been integrated into a coherent legal protection framework. Following the enactment of the PDP Law, the principal challenge is no longer simply the existence of a legal vacuum but rather the gap between the comprehensiveness of legal norms and their effective implementation in practice.

Although the PDP Law provides a stronger legal foundation, the effectiveness of personal data protection depends substantially on implementation capacity. Limited understanding among the public and organizations concerning personal data rights and obligations may prevent legal norms from being translated into effective operational procedures. Weak technological safeguards, inadequate oversight, ineffective internal governance, and deficient incident-response mechanisms may further undermine protections that are formally established by law. Personal data protection mechanisms

²² Idden Aryasatya et al., “Analisis Kebijakan Keamanan Siber Indonesia Dalam Strategi Nasional Keamanan Siber,” *Jurnal Impresi Indonesia* 5, no. 3 (2026): 1411–27, <https://doi.org/10.58344/jii.v5i3.7656>.

²³ Agusta, “Perlindungan Data Pribadi Penerima Pinjaman Dalam Transaksi Pinjam Meminjam Uang Berbasis Teknologi Informasi.”

²⁴ Purnama and Alhakim, “Pentingnya UU Perlindungan Data Pribadi Sebagai Bentuk Perlindungan Hukum Terhadap Privasi Di Indonesia.”

²⁵ Suharyanti and Sutrisni, “Urgensi Perlindungan Data Pribadi Dalam Menjamin Hak Privasi Masyarakat.”

²⁶ Buana, “Perlindungan Hukum Terhadap Data Pribadi Kepada Pemilik Data Pribadi Dalam Penyelenggaraan Jasa Fintech Peer To Peer Lending.”

²⁷ Saputra et al., “Penerapan Privasi Dan Etika Di Era Digital Dalam Perlindungan Data Pribadi.”

should therefore be understood as an integrated combination of legal compliance, institutional governance, technical security, and the empowerment of data subjects.

The historical development of data protection law in Germany and Sweden following the emergence of computerization in the 1970s demonstrates that data protection regulations developed in response to the risks that technological advances posed to individual freedoms and rights.²⁸ This development subsequently contributed to the emergence of modern data protection standards in various jurisdictions. Global principles, including those reflected in the General Data Protection Regulation (GDPR), may therefore serve as comparative benchmarks, particularly with respect to transparency, purpose limitation, data minimization, integrity, and confidentiality. Nevertheless, international standards do not supersede the PDP Law. As Indonesia's national legal framework, the PDP Law remains the primary legal basis for assessing the adequacy of personal data protection mechanisms in Indonesia.

In principle, personal data protection mechanisms in Indonesia have acquired a robust normative foundation through Law No. 27 of 2022 on Personal Data Protection. The adequacy of these mechanisms depends on whether personal data processing is based on a valid legal ground, whether data subjects can effectively exercise their rights, whether data controllers and processors fulfill their obligations concerning security and confidentiality, and whether effective accountability and redress mechanisms are available when violations occur. Although the PDP Law establishes relatively comprehensive legal standards, effective protection cannot be achieved solely through the existence of legal norms. Consistent implementation, strengthened regulatory oversight, enhanced legal and digital literacy, robust technological safeguards, and effective incident-response and remediation mechanisms are equally essential. Accordingly, efforts to strengthen personal data protection in Indonesia should focus on the effective realization of individual rights, ensuring that the PDP Law functions not merely as a regulatory instrument but as an effective legal mechanism for safeguarding the security, confidentiality, and individual control of personal data within the digital ecosystem.

4. CONCLUSION

The security and confidentiality of personal data constitute integral components of the right to personal privacy and are constitutionally grounded in Article 28G(1) of the 1945 Constitution of the Republic of Indonesia. This position is consistent with the Constitutional Court's affirmation that personal data protection is inseparable from the constitutional right to personal protection. Furthermore, Law No. 27 of 2022 on Personal Data Protection (the PDP Law) establishes a comprehensive legal framework

²⁸ Collin J. Bennett, *Regulating Privacy: Data Protection and Public Policy in Europe and the United States* (Cornell University Press, 1992).

governing lawful bases for data processing, data subject rights, the obligations of data controllers and processors, data security and confidentiality, and accountability mechanisms.

The principal challenge is therefore no longer the absence of legal norms but the consistency of their implementation and the effectiveness of enforcement. This study contributes to the literature by reinforcing a rights-based approach to personal data governance, emphasizing that data protection should be oriented toward safeguarding individual rights rather than merely ensuring technical or administrative compliance. Nevertheless, the study is limited by its normative approach, which does not empirically measure the effectiveness of implementation in practice.

Accordingly, personal data protection policies should strengthen regulatory oversight, public and institutional awareness, technological security, and accessible redress mechanisms. Future research should adopt socio-legal or empirical approaches to examine the gap between the normative framework established by the PDP Law and its implementation in practice, thereby providing a more comprehensive assessment of the effectiveness of personal data protection in Indonesia.

REFERENCES

Journals

- Agusta, Hendrawan. "Perlindungan Data Pribadi Penerima Pinjaman dalam Transaksi Pinjam Meminjam Uang Berbasis Teknologi Informasi: Peer To Peer Lending." *Jurnal Hukum & Pembangunan* 50, no. 4 (2020): 780–809. <https://doi.org/10.21143/jhp.vol50.no4.1029>.
- Alvember, Mario, and Dyah Permata Budi Asri. "Analisis Keamanan Data Pribadi Konsumen Terhadap Regulasi Pencantuman Nomor Induk Kependudukan Untuk Registrasi Nomor Telepon." *Arus Jurnal Sosial Dan Humaniora* 5, no. 2 (2025): 3017–26. <https://doi.org/10.57250/ajsh.v5i2.1590>.
- Amalia, Rina, Dimas Yoga, and Putri Maharani. "Legal Protection of Personal Data in the Digital Era: Challenges and Regulatory Framework in Indonesia." *Journal of Lex et Justitia* 2, no. 1 (2026): 50–65. <https://doi.org/10.67171/mnrwww36>.
- Arthaputri, Sylvia Faradina Amandasari. "Perlindungan Data Pribadi Sebagai Bentuk Perwujudan Cyber Security: Studi Komparatif Indonesia Dan Singapura." *Dinamika: Jurnal Ilmiah Hukum* 30, no. 1 (2024).
- Aryasatya, Idden, Stanislaus Riyanta, and Eko Daryanto. "Analisis Kebijakan Keamanan Siber Indonesia Dalam Strategi Nasional Keamanan Siber." *Jurnal Impresi Indonesia* 5, no. 3 (2026): 1411–27. <https://doi.org/10.58344/jii.v5i3.7656>.
- Fachri, Faisal, Ariy Khaerudin, and Nourma Dewi. "Protection of Digital Privacy Rights as a Human Right Against Personal Data Misuse in Indonesia." *Journal of International Islamic Law, Human Right and Public Policy* 4, no. 3 (2026): 1332–37. <https://doi.org/10.5281/ZENODO.21853686>.

- Hanita, Margaretha. "Transformasi Ketahanan Wilayah Pada Era Digital: Peran Kepemimpinan Digital Dalam Membangun Smart City Di Kota Pariaman Sumatera Barat." *Jurnal Ketahanan Nasional* 29, no. 2 (2023): 178–98. <https://doi.org/10.22146/jkn.86067>.
- Jebaru, Reginaldus Arfan, and Men Wih Widiatno. "Perlindungan Hukum Bagi Prosesor Data Pribadi Dalam Melaksanakan Pemrosesan Data Pribadi Menggunakan Aplikasi Sistem Informasi Kependudukan: Penelitian." *Jurnal Pengabdian Masyarakat Dan Riset Pendidikan* 4, no. 3 (2026): 19564–72. <https://doi.org/10.31004/jerkin.v4i3.5184>.
- Mardiyati, Siti. "Konstitusionalitas Perlindungan Data Pribadi Sebagai Bagian Dari Hak Atas Rasa Aman." *Consensus: Jurnal Ilmu Hukum* 4, no. 2 (2025): 221–33. <https://doi.org/10.46839/consensus.v4i2.1758>.
- Pakaya, Putri Regina S., Suwitno Yutye Imran, and Apripari Apripari. "Dampak Penyebaran Data Pribadi Melalui Media Digital Terhadap Perlindungan Hak Privasi." *Jurnal Hukum Bisnis* 15, no. 1 (2026): 17–26. <https://doi.org/10.47709/jhb.v15i01.7594>.
- Pakpahan, Jonathan Matthew. "Kesadaran Urgensi Peran Pengendali Dan Prosesor Data Pribadi Dalam Rangka Pelindungan Data Pribadi Individu Berdasarkan Undang-Undang Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi." *Jurnal Hukum To-Ra : Hukum Untuk Mengatur Dan Melindungi Masyarakat* 10, no. 1 (2024): 119–37. <https://doi.org/10.55809/tora.v10i1.331>.
- Purnama, Thiara Dewi, and Abdurrahman Alhakim. "Pentingnya UU Perlindungan Data Pribadi Sebagai Bentuk Perlindungan Hukum Terhadap Privasi Di Indonesia." *Jurnal Komunitas Yustisia* 4, no. 3 (2021): 1056–64. <https://doi.org/10.23887/jatayu.v4i3.44370>.
- Remanu, Alifah Jasmine Kallista, Bella Ola Shakira, Najwa Adhwa Ramadhani, Zahra Hanifah Salma, and Muhammad Prakoso Aji. "Analisis Transformasi Digital Pelayanan Publik Identitas Kependudukan Digital (IKD) Dalam Implementasi Digital Governance Di Suku Dinas Kependudukan Dan Pencatatan Sipil Jakarta Selatan." *Jurnal Kolaboratif Sains* 9, no. 5 (2026): 3691–707. <https://doi.org/10.56338/jks.v9i5.10899>.
- Saputra, Beni Andrian, Eni Kurnia, Maulidatur Rahmah, and Titin Sumarni. "Penerapan Privasi Dan Etika Di Era Digital Dalam Perlindungan Data Pribadi." *Musytari: Neraca Manajemen, Akuntansi, Dan Ekonomi* 5, no. 9 (2024). <https://ejournal.warunayama.org/index.php/musytarineraca/article/view/3570/3351>.
- Tanuwidjaja, Carissa. "Protection of Personal Data in the Digital Era: Legal Analysis and Implementation Challenges in Indonesia." *Journal of Legal Studies Judex Praetor* 2, no. 1 (2026): 1–19. <https://doi.org/10.35671/judex.v2i1.174>.
- Utami, Sal Sabila Khoirotunnisa. "Personal Data Protection and Its Regulatory Frameworks Under Cyber Law." *Domus Legalis Cogitatio* 1, no. 2 (2024): 175–93. <https://doi.org/10.24002/dlc.v1i2.9894>.

Proceedings

Suharyanti, Ni Putu Noni, and Ni Komang Sutrisni. "Urgensi Perlindungan Data Pribadi Dalam Menjamin Hak Privasi Masyarakat." *Prosiding Seminar Nasional Fakultas Hukum Universitas Mahasaraswati Denpasar* (Denpasar) 1, no. 1 (2020): 119–34. <https://e-journal.unmas.ac.id/index.php/psnfh/article/view/2395>.

Thesis

Buana, Sandy Ekki Wiratama. "Perlindungan Hukum Terhadap Data Pribadi Kepada Pemilik Data Pribadi Dalam Penyelenggaraan Jasa Fintech Peer To Peer Lending." Universitas Islam Indonesia, 2022. <https://dspace.uii.ac.id/handle/123456789/39314>.

Books

Bennett, Collin J. *Regulating Privacy: Data Protection and Public Policy in Europe and the United States*. Cornell University Press, 1992.

Web Pages

Anastasya, Sinta. "Kebocoran Data 15 Juta Pengguna E-Commerce: Ancaman Nyata Keamanan Digital Di Indonesia." Kompasiana, Kompasiana, 2026. https://www.kompasiana.com/sintaanastasya0349/695cb04aed6415211e61ad44/kebocoran-data-15-juta-pengguna-e-commerce-ancaman-nyata-keamanan-digital-di-indonesia#goog_rewarded.