

NAVIGATING THE INSTITUTIONAL VACUUM OF PERSONAL DATA PROTECTION AND PUBLIC TRUST IN INDONESIA

Elvinna Aurellia Arya Putri Machmudi*

UIN Sunan Ampel, Surabaya, East Java, Indonesia

Email: vinamahmudi23@gmail.com

Article Info

Keyword:

Personal Data
Protection,
Independent
Supervisory Agency,
Legal Certainty.

Abstract

This study aims to examine the urgency and institutional prospects for establishing an independent personal data protection supervisory agency, based on the mandate of Article 58 of Law Number 27 of 2022 in Indonesia. The main problem in Indonesia today is driven by the rapid advancement of information systems, which increases the risk of data leaks. The method used in writing this article is normative legal research through legislative and conceptual approaches. Legal materials were obtained through literature studies and then discussed descriptively and qualitatively. The research results clearly demonstrate that the absence of a dedicated supervisory agency has created an institutional vacuum. As a result, legal quality is severely weakened, public accountability is low, and oversight patterns are partial, thus prone to conflicts of interest. However, various global comparisons demonstrate the role of independent institutions in safeguarding data sovereignty and enhancing public trust. In conclusion, the establishment of an independent personal data supervisory agency is an absolute constitutional guarantee to protect the privacy rights of every citizen, as guaranteed by Article 28G of the 1945 Constitution. Based on the results of an in-depth analysis, it is recommended that the president, as head of state, immediately ratify this independent supervisory agency to fill legal gaps, strengthen the enforcement of regulations, and provide fair, firm, transparent, and inclusive legal certainty for all personal data governance within the national digital ecosystem in a sustainable manner.

Page: 113-123

* Corresponding Author.

Article history:

Received: February 12, 2025; Received in revised form: October 02, 2025; Available online: November 30, 2025.

Copyright © 2025 The author(s).

Published by International Journal of Law Dynamics Review. This is an open access article under the CC BY-NC 4.0 license (<https://creativecommons.org/licenses/by-nc/4.0>).

Introduction

The development of information and communication technology has brought major changes to various aspects of people's lives, shifting daily activities such as online shopping, online schooling, banking transactions, health services, and social media to rely heavily on the collection and processing of personal data (Soemitro et al., 2023). Personal data constitutes an essential asset containing crucial information—including full names, gender, National Identification Numbers (NIK), and residential addresses—that can be utilized for various purposes by individuals and institutions (Sholichah & Rumaisa, 2018). This digital shift directly interfaces with the 1945 Constitution, where Article 28 D paragraph (1) guarantees the right to the protection of one's personal self, family, honor, dignity, and property, while Article 28 H paragraph (4) stipulates that private property rights cannot be arbitrarily taken away by anyone. Based on these constitutional provisions, the state is strictly obliged to provide adequate physical, mental, and data protection to individuals and their possessions (Kholik et al., 2024). However, without optimal safeguards, the ease of access and rapid dissemination of information pose severe risks of data misuse, as evidenced by the alarming escalation of personal data breaches in Indonesia, with an estimated 94.22 million accounts leaked between 2020 and 2024.

This widespread misuse of personal data has a serious impact on human rights, particularly the right to privacy guaranteed under Article 28G Paragraph 1 of the 1945 Constitution. Historically, before a comprehensive legal umbrella was enacted in Indonesia, personal data protection was regulated fragmentarily through various sector-specific legislations, including Law Number 39 of 1999 concerning Human Rights, Law Number 11 of 2008 concerning Electronic Information and Transactions (ITE), Law No. 14 of 2008 concerning Public Information Disclosure, and Government Regulation No. 71 of 2019 concerning the Implementation of Electronic Systems and Transactions (Wachdin et al., 2024). To consolidate these dispersed regulations and recognize the growing importance of data privacy, the state enacted Law Number 27 of 2022 concerning Personal Data Protection (PDP Law). The PDP Law represents an important milestone designed to provide a stronger legal umbrella for citizens' rights regarding the collection, use, and dissemination of personal data, while simultaneously emphasizing that rigorous and centralized supervision is vital for this protection to be implemented effectively (Syailendra et al., 2024).

A crucial aspect of Law Number 27 of 2022 concerning Personal Data Protection is the specific mandate in Article 58, paragraph 2, and Article 53, paragraph 3, which dictates that the implementation of personal data protection must be carried out by a specialized Personal Data Protection Agency established by the president. This agency is structurally designed to be an independent authority capable of executing supervisory, law enforcement, and dispute resolution functions; yet, because the agency has not been established to date, a critical institutional vacuum has emerged (Dharma & Wiraguna, 2026). Without this specialized institution, current supervision remains sectoral and partial, depending on certain ministries that are structurally prone to conflicts of interest. This situation exposes severe structural weaknesses in the implementation of the PDP Law, failing to guarantee legal certainty for the public. In the global context, previous models demonstrate that independent bodies, such as the Data Protection Authority (DPA) in the European Union and the Personal Data Protection Commission (PDPC) in Singapore, successfully increase law enforcement, strengthen public trust, and solidify national data sovereignty, proving that Indonesia urgently needs a similar standalone institution to address digital age challenges (Dharma & Wiraguna, 2026).

To resolve these institutional limitations, this situation raises two central problems: first, the inherent weakness of the sectoral monitoring system, which lacks clear coordination and enforcement powers, rendering personal data protection sub-optimal; and second, the

direct urgency of establishing a dedicated personal data protection agency as an independent institution to enforce compliance and provide absolute legal certainty (Cantik & Rahmahani, 2026). Therefore, the overarching objective of this research is to evaluate the constitutional urgency and institutional prospects of establishing this independent personal data protection agency based on the statutory mandates of Article 58 of the PDP Law. Ultimately, the significance of this study lies in systematically identifying these institutional gaps and structural vulnerabilities, outlining how the immediate presence of this independent agency is not merely an administrative necessity but a vital constitutional guarantee to safeguard the privacy rights of citizens in the contemporary digital era.

Research Method

This study uses a normative legal research method, which is research that focuses on reviewing applicable laws and regulations and legal doctrines (Diantha, 2019). The approach used is a legislative approach by examining the 1945 Constitution, Law Number 27 of 2022 concerning Personal Data Protection, and other related regulations (Marzuki, 2017), as well as a conceptual approach by examining the principles of personal data protection, the right to privacy, and the urgency of establishing an independent institution (Ibrahim, 2013). The legal sources consist of primary legal materials in the form of legislation, secondary legal materials in the form of literature, journals, and expert opinions. The technique of collecting legal materials was carried out through a literature study, while data analysis was carried out descriptively and qualitatively by describing, interpreting, and assessing existing legal norms to conclude the urgency of establishing a Personal Data Protection Agency in Indonesia.

Results and discussions

Weaknesses of the Personal Data Protection Supervision System Without a Special Agency

Personal data protection has become a crucial issue in contemporary society as personal data evolves into a valuable asset frequently exploited by various parties for business and political interests. Although the enactment of Law Number 27 of 2022 concerning Personal Data Protection (PDP Law) represents a significant step to provide a clearer legal umbrella for citizens, monitoring its implementation remains a fundamental problem because the law cannot fully guarantee effective monitoring without a special, independent, and fully authorized institution (Suwondo, 2023). Under Article 58, the president is mandated to establish a personal data protection agency, ratified in 2024, which was structurally designed to be placed as a unit within the Ministry of Communication and Information Technology for a six-month to one-year transition period before operating as an independent institution. However, because this personal data protection agency remains under discussion without any signs of imminent ratification, this institutional delay results in the complete absence of an authority that functions optimally in terms of prevention, supervision, and dispute resolution related to personal data leaks (Hernowo, 2025).

In principle, personal data protection agencies play an important role in enforcing compliance with data protection standards and obligations by data controllers and processors, meaning that without such a centralized body, the implementation of the PDP Law faces major obstacles to running optimally, including in ensuring that the rights of data subjects are fulfilled. This absence of a special agency results in weak law enforcement, as personal data violations are often bundled by sectoral institutions—such as the Ministry of Communication and Information Technology or standard law enforcement agencies—which actually have limited authority and remain bound by certain bureaucratic interests (Irfandi, 2026). Consequently, the capacity of law enforcement agencies to handle data crime cases is still

limited, while coordination between agencies remains structurally weak. Furthermore, the absence of a compensation mechanism for victims and the perception of unfair treatment in prosecution further undermine public trust, leaving many data breach cases unresolved and giving the impression that personal data breaches are not considered serious crimes in Indonesia, which weakens the deterrent effect, encourages digital service providers not to make security improvements, and undermines the state's legitimacy in guaranteeing the digital rights of the people (Joko Nursasih & Sri Ratnaning Dhumillah, 2026).

Concurrently, the level of accountability and transparency of oversight is remarkably low without a specific agency to handle personal data protection violations, as sectoral agencies are often more oriented towards protecting their own institutions than providing maximum protection for data subjects. This institutional self-preservation results in the public losing access to clear information about how data violation cases are handled; in fact, it is not uncommon for cases to be resolved behind closed doors, causing public distrust of the government's commitment to protecting personal data. Furthermore, relying on non-independent institutions opens up structural opportunities for the abuse of power, directly introducing the potential for an individual's personal data to be manipulated or exploited for political or commercial purposes by uncoordinated actors (Nafisah & Diniyanto, 2024).

Weak oversight without a specialized agency also results in low public awareness of the importance of protecting personal data, given that public education is one of the strategic functions of an oversight agency that is currently spread across various agencies without coordination, resulting in education programs that are unfocused and do not reach all levels of society. As a result, the public remains highly vulnerable to data misuse due to a lack of understanding of their rights and obligations as data subjects, making it difficult to establish an effective complaint mechanism. Consequently, people are often confused about where to report data misuse or leaks, a situation that differs completely from countries that already have special agencies to handle data protection, such as the European Union, Singapore, Norway, the United Kingdom, the United States, Thailand, and many others, where citizens experiencing a data breach can immediately report it and obtain a clear resolution. Conversely, the current situation in Indonesia makes people tend to be passive or even not report violations because the existing procedures are complicated and the results remain highly uncertain (Natamiharja, 2018).

The Urgency of Establishing a Personal Data Protection Agency

Personal data protection guarantees the rights and freedoms of individuals over their data, ensuring that it is not violated by other parties, whether individuals, agencies, or institutions, without legal authority in accordance with the provisions of the law. The concept of personal data protection emphasizes that everyone has the right to determine their own fate, such as whether or not to share their data. If they agree to share their data, they have the right to determine the conditions that must be met within a community (Ayunda, 2022). Personal data protection needs to be accompanied by an institution that plays a role in monitoring its implementation. The establishment of a personal data protection supervisory agency shows that the state plays an important role in ensuring the security and protection of people's personal data. In addition, the existence of a personal data protection supervisory agency can provide legal certainty in the application of regulations related to personal data protection. The establishment of a personal data protection supervisory agency can ensure that the confidentiality of personal data in both public and private institutions is maintained (Syafra et al., 2022).

Several factors underlie the urgency of establishing a personal data protection agency, one of which is to ensure that personal data protection regulations can be effectively implemented. Personal data is a right of every person that is protected by the constitution, so that personal data protection is not only aimed at protecting individual information, but also at

guaranteeing the basic rights and freedoms of every person. This is in line with the provisions of Article 28G paragraph (1) of the 1945 Constitution of the Republic of Indonesia, which states that every person has the right to protection of their personal self, family, honor, dignity, and property under their control, and has the right to feel safe and protected from threats of fear in exercising their basic rights. In addition, Article 28H paragraph (4) of the 1945 Constitution also guarantees the right of every person to personal property that cannot be arbitrarily taken by anyone. Based on these provisions, the state has a constitutional obligation to take concrete steps to protect every individual, both in terms of their life and body as well as everything they own, including personal data. In this context, the establishment of a personal data protection supervisory agency is a fundamental principle in ensuring responsible personal data management. Practices in various countries in Asia and Europe show that the existence of an independent supervisory agency plays an important role in ensuring that personal data protection is implemented consistently, effectively, and in accordance with applicable legal principles (Neta et al., 2022).

Supervision and law enforcement regarding the implementation of personal data protection regulations in Indonesia are still relatively weak. Personal data protection is still sectoral in nature, so supervision of its implementation is carried out separately according to each sector. For example, the banking sector is under the supervision of Bank Indonesia (BI) or the Financial Services Authority (OJK). In addition, existing personal data protection regulations are still general in nature and tend to only explain the concept of personal data protection normatively without integrated supervision and law enforcement mechanisms (Admiral & Pauck, 2023). This condition is reinforced by a statement from the National Consumer Protection Agency of the Republic of Indonesia (BPKN-RI), which states that Indonesia still faces a high number of data violations, indicating that the personal data protection supervision and law enforcement system is not yet functioning optimally.

The urgency of establishing a personal data protection agency is also growing in line with the increasing number of subjects of personal data protection in Indonesia. Indonesia is one of the countries with the largest population in the world, with the Ministry of Home Affairs estimating that Indonesia's population in June 2025 will reach 286,693,693. This means that there are approximately 286.6 million subjects of personal data protection whose confidentiality must be guaranteed by the state. As people's activities in the virtual world increase, whether in the economic, social, or public service sectors, the risk of misuse and theft of personal data also increases. However, this increase in digital activity has not been matched by adequate supervision and law enforcement, making the public increasingly vulnerable to personal data breaches. This weak supervision and law enforcement is also related to the large amount of personal data that must be protected, while existing supervisory agencies, such as the OJK and other government agencies, do not specifically and exclusively carry out the function of personal data protection (Kriswandaru et al., 2024).

In addition to the increasing number of subjects of personal data protection, the complexity of data protection is also influenced by the large number of controllers and processors of personal data in Indonesia. Controllers of personal data include individuals, public institutions, non-public institutions, or private parties/corporations, and even international organizations. The large number of actors involved in the control and processing of personal data requires serious, focused, and continuous supervision. If supervision is only carried out by institutions that do not specifically focus on personal data protection and supervision, the main objective of personal data protection will be difficult to achieve (Adytia et al., 2024; Wachdin et al., 2024). Furthermore, the scope of personal data protected is also very broad, because personal data is divided into two categories, namely general personal data and special personal data. General personal data includes information that can be used to identify individuals, such as full name, gender, nationality, and religion. Meanwhile, special personal data includes sensitive data, such as health data, biometric data, genetic data, sexual

life or sexual orientation, political views, criminal records, child data, personal financial data, and other types of data as stipulated in the provisions of laws and regulations. Based on these conditions, it can be concluded that the supervision of controllers and processors of personal data has a very broad scope, both in terms of the number of legal subjects and the types of data objects protected. Therefore, without an institution that specifically focuses on the protection and supervision of personal data, the achievement of the main objectives of personal data protection will face various serious obstacles (Advent Pateh et al., 2022).

Countries around the world have established personal data protection supervisory agencies as part of their efforts to guarantee the privacy rights of their citizens, one of which is the United Kingdom. In this country, personal data protection is supervised by the Information Commissioner's Office (ICO), an independent agency responsible to the UK Parliament and selected and appointed by parliament. The personal data protection framework in the United Kingdom is regulated by the Data Protection Act 1998 and reinforced through the implementation of the General Data Protection Regulation (GDPR). This regulation strictly regulates the processing of personal data, including restrictions on the transfer of personal data outside Europe if the destination country does not have an equivalent level of data protection. This principle of equivalence of protection affirms that personal data transfers can only be carried out if the recipient country is able to guarantee equivalent protection. The GDPR not only focuses on handling data breaches after they occur, but also emphasizes preventive measures, such as data protection impact assessments and the implementation of privacy by design. This approach is considered relevant for adoption in Indonesia because it can strengthen the data protection system in a preventive and sustainable manner (Khair & Wiraguna, 2025).

In Asia, Hong Kong has been one of the pioneers in establishing a regulatory framework for personal data protection through the enactment of the Personal Data (Privacy) Ordinance (PDPO) in 1995, which underwent significant changes in 2012. The implementation and supervision of personal data protection in Hong Kong is carried out by the Privacy Commissioner for Personal Data (PCPD), who reports directly to the Chief Executive. The principles of personal data protection in the PDPO comprehensively regulate the process of collecting, using, storing, and disclosing personal data. Data collection must be carried out for legitimate and relevant purposes, the use and disclosure of data must be in accordance with the original purpose and require the consent of the data subject, and the quality of the data must be maintained so that it remains accurate and up to date. In addition, the PDPO also limits the period of data storage by third parties, requires data controllers to protect data from unauthorized access, and emphasizes the principle of transparency through the obligation of data controllers to publish their privacy policies (Siti Yuniarti et al., 2023).

Meanwhile, Singapore passed the Personal Data Protection Act (PDPA) in 2012 as the main legal basis for personal data protection. Oversight of the implementation of the PDPA is carried out by the Personal Data Protection Commission (PDPC), which is under the responsibility of the Minister for Communications and Information. The PDPC plays a strategic role in raising public awareness of personal data protection, providing policy input to the government, representing Singapore in international cooperation in the field of data protection, and conducting research, surveys, and education related to personal data protection. In addition to its supervisory functions, the PDPC also issues various regulations and technical guidelines for organizations or parties that collect and process personal data. The PDPA requires any party that collects data to obtain consent from individuals before using or disclosing personal data, and to ensure that personal data transferred overseas continues to receive a level of protection equivalent to the data protection standards applicable in Singapore (Dewi et al., 2019).

Finally, in Malaysia, personal data protection is regulated by Act No. 709 of 2010, known as the Personal Data Protection Act 2010. This law regulates the protection of

personal data limited to the commercial sector, while the public sector is not included in the scope of protection regulated. However, Malaysia has established a personal data protection supervisory agency called the Personal Data Protection Commissioner, which is under the responsibility of a minister. This agency plays an important role in ensuring the implementation and enforcement of personal data protection provisions in Malaysia. The supervisory functions include advising the minister on national policies in the field of personal data protection, enforcing and maintaining personal data protection laws against any violations, and encouraging and facilitating associations or bodies representing data users to develop and disseminate codes of practice. In addition, the supervisory agency is also tasked with monitoring developments in personal data processing, overseeing the level of compliance with the provisions of the Personal Data Protection Act, establishing cooperation with external parties outside Malaysia for the sake of personal data protection, and carrying out other tasks mandated by laws and regulations related to personal data protection (Anand et al., 2020).

The positive aspects that Indonesia can use as a reference in establishing a Personal Data Supervisory Agency can be traced to the institutional practices of personal data protection in various countries, as described above. One of the main aspects is the principle of institutional independence, which allows the supervisory agency to operate independently from political influence and other institutional interests so that it can make decisions that are oriented towards the public interest. This principle is important so that the functions of supervision and law enforcement can be carried out objectively and professionally, and in line with the provisions of Article 58 paragraph (2) of the Personal Data Protection Law, which requires the independence of the supervisory agency even though it is formed under the government (Yuniarti, 2022). In addition to independence, firm and consistent law enforcement is a crucial aspect to ensure the protection of individuals' personal data and encourage compliance by data controllers and processors with applicable regulations. Furthermore, international cooperation needs to be actively developed through coordination with supervisory agencies in other countries to anticipate the cross-border flow of personal data and ensure that data protection standards in Indonesia are in line with global practices (Arifin et al., 2021).

The establishment of a personal data protection supervisory authority in Indonesia is considered more appropriate if it uses an independent institution model formed by the state through a legal basis in the form of a law. The development of institutions in Indonesia has shown rapid progress, beyond the institutions that are explicitly regulated in the 1945 Constitution of the Republic of Indonesia, which distinguishes the branches of state power in the legislative, executive, and judicial fields. According to Jimly Asshiddiqie, since the 1945 Constitution changed, it can be said that the 1945 Constitution of the Republic of Indonesia adheres to the separation of powers by developing a more functional check and balance mechanism, which means that state institutions can fill each other's power vacuums so that the system can run smoothly. Since the amendment of the 1945 Constitution to the present, many state institutions have been formed independently through various laws and regulations (state auxiliary agencies) that have influenced the Indonesian constitutional system. The establishment of institutions is based on legislation, which means that the formation of an institution is still sectoral in nature. If there is a need to form an institution, provisions governing the process of establishing that institution will be drafted (Alkahfi Setiawan, 2022).

The formation of new state institutions, including oversight bodies, is driven by various structural and contextual factors. One key factor is the declining credibility of existing state institutions due to strong evidence and assumptions of deep-seated, systemic corruption that is difficult to eradicate. Furthermore, the weak independence of state institutions due to their attachment to particular interests makes them vulnerable to intervention by political and economic forces. Internal and external weaknesses faced by state institutions also contribute

to their inability to carry out strategic tasks, particularly during the transition to a more mature democratic system. On the other hand, global influences indicate a tendency in various countries to establish additional state institutions, such as state support institutions or oversight bodies, in response to the need for institutional reform, as existing institutions have become part of the system in need of improvement. Furthermore, pressure from international institutions has also driven the formation of these institutions as a crucial prerequisite for entering a new era of democratization that demands transparent and accountable governance (Arsyad et al., 2026).

The establishment of a personal data protection authority is a necessary step to fulfill the basic rights of citizens. The right to privacy must be protected by the state through a personal data protection authority. In addition, the establishment of a personal data protection authority is intended to create a fair mechanism for supervision and law enforcement in the field of personal data protection and enable the government to carry out the mandate given by Law Number 27 of 2022 concerning Personal Data Protection (Badar et al., 2023). The process of establishing non-integrated state institutions can result in overlapping authorities between existing institutions, thereby causing inefficiency in government administration. The establishment of auxiliary state organs in Indonesia can be applied to personal data protection agencies. However, it is necessary to regulate how this independence is achieved. One comparison with personal data protection agencies can be taken from the example of the personal data protection agency established by the EU GDPR. The EU GDPR regulates the requirements for the independence of a personal data protection agency (Lynskey, 2017).

Conclusion

This research evaluates the constitutional urgency and institutional prospects of establishing an independent personal data protection authority in Indonesia as mandated by Article 58 of Law Number 27 of 2022. The findings demonstrate that the current absence of this specialized agency creates a critical institutional vacuum, rendering data supervision fragmented, sectoral, and highly prone to bureaucratic conflicts of interest. Theoretically, these insights enrich domestic administrative law discourses by illustrating how state auxiliary organs secure constitutional privacy rights under Article 28G. Practically, establishing this independent agency remains imperative to eliminate enforcement vulnerabilities and restore public trust.

The unique scientific contribution of this research lies in its comprehensive comparative framework, drawing structural lessons from independent global models like the United Kingdom's ICO and Singapore's PDPC to design an ideal institutional blueprint. However, this study is limited by its primary focus on statutory analysis and initial implementation obstacles. Future research should expand this dataset by conducting empirical assessments of institutional readiness across various critical public sectors. Ultimately, immediate presidential ratification of this standalone authority is vital to safeguard national data sovereignty and guarantee absolute legal certainty within the comprehensive contemporary Indonesian digital ecosystem.

Declaration of AI and AI-Assisted Technologies in the Writing Process

During the preparation of this manuscript, the author employed Artificial Intelligence (AI)-assisted technology, specifically ChatGPT (OpenAI). The author is solely responsible for the final content, interpretation, and conclusions presented in this publication.

CRediT Authorship Contribution Statement

1. **Elvinna Aurellia Arya Putri Machmudi:** Conceptualization, Data Curation, Formal Analysis, Methodology, Writing – Original Draft, Writing – Review & Editing, Resources, and Translation.

Declaration of Competing Interest

The author declares that no financial, professional, or personal conflict of interest could affect the research process, interpretation of findings, or publication of this article.

Acknowledgments

The author would like to express his deepest gratitude and sincere appreciation to his beloved parents for their endless prayers, unconditional love, unwavering encouragement, and priceless sacrifice throughout his academic journey and completion of this research.

Data Availability Statement

Data supporting the findings of this study are available from the relevant authors upon reasonable request via email at **vinamahmudi23@gmail.com**. All materials and sources used in this study were obtained from relevant academic literature and library-based scientific resources.

Funding Statement

This research was conducted independently and does not receive any financial support, grants, or special funding from government agencies, private organizations, or other funding agencies.

Ethical Approval Statement

The author emphasized that this research was conducted in accordance with established academic and research ethics standards. As a library-based study, this study did not involve human participants, personal data, or identifiable respondent information. Therefore, formal ethical approval is not required for the implementation of this research.

Bibliography

- Admiral, A., & Pauck, M. A. (2023). Unveiling the Dark Side of Fintech: Challenges and Breaches in Protecting User Data in Indonesia's Online Loan Services. *Lex Scientia Law Review*, 7(2), 995–1048. <https://doi.org/10.15294/LESREV.V7I2.77881>
- Advent Pateh, Anugrah Putra Ramadhan, Popo Hartono, Nirmala Sari Dwi S.P, & Theresia Anita Christiani. (2022). Proposed Concept of Establishing an Oversight Institution in the Implementation of Personal Data Protection to Achieve Beneficial Value for Legal Purposes. *International Journal of Social Science And Human Research*, 05(12), 5863–5870. <https://doi.org/10.5281/ZENODO.7472574>
- Adytia, N. A. P., Arief, S., & Astesa, D. (2024). Regulatory Arrangements and Utilization of Artificial Intelligence (AI) in Realizing Personal Data Protection in Indonesia. *KnE Social Sciences*, 9(1), 920–927–920–927. <https://doi.org/10.18502/KSS.V8I21.14807>
- Alkahfi Setiawan, S. (2022). Ambiguitas Putusan Mahkamah Konstitusi Republik Indonesia Dalam Perkara Nomor 91/PUU/MK-VXIII/2020. *WELFARE STATE Jurnal Hukum*,

- 1(1), 1–16. <https://doi.org/10.56013/WELFARESTATE.V1I1.1549>
- Anand, G., Hernoko, A. Y., & Dharmadji, A. G. (2020). The Urgency of Enacting Personal Data Protection Law as A Patronage from The Development of Communication and Information Technology in Indonesia. *PERSPEKTIF: Kajian Masalah Hukum Dan Pembangunan*, 25(1), 54–62. <https://doi.org/10.30742/PERSPEKTIF.V25I1.750>
- Arifin, R., Kambuno, J. A., Waspiyah, & Latifiani, D. (2021). Protecting the Consumer Rights in the Digital Economic Era: Future Challenges in Indonesia. *Jambura Law Review*, 3(Special Issues April), 135–160. <https://doi.org/10.33756/JLR.V3I0.9635>
- Arsyad, N., Ode Husen, L., Hasyim, S., & Kahar Muzakkir, A. (2026). The Nature of Mechanism for Enforcing the Ethics and Honor of State Administrators as a Preventive Measure for Corrupt Practices. *Cogent Social Sciences*, 12(1), 1–17. <https://doi.org/10.1080/23311886.2026.2620142>
- Ayunda, R. (2022). Personal Data Protection to E-Commerce Consumer: What Are the Legal Challenges and Certainties? *LAW REFORM*, 18(2), 144–163. <https://doi.org/10.14710/LR.V18I2.43307>
- Badar, E. S., Fauzi, A., & Jazuli, A. (2023). Personal Data Protection Policy in Law Number 27 Of 2022 in The Perspective of Positive Law and Islamic Law. *Hukum Islam*, 23(1), 61–74. <https://doi.org/10.24014/JHI.V23I1.20465>
- Cantik, D., & Rahmahani, A. P. (2026). The Urgency of Establishing a Supervisory Agency for the Implementation of Personal Data Protection in the Implementation of the Personal Data Protection Law. *International Journal of Science and Environment (IJSE)*, 6(1), 300–308. <https://doi.org/10.51601/IJSE.V6I1.332>
- Dewi, S., Walters, R., Trakman, L., & Zeller, B. (2019). The Role of International Mediation in Data Protection and Privacy Law - Can It be Effective? *SSRN Electronic Journal*, 30(61), 19–77. <https://doi.org/10.2139/SSRN.3462113>
- Dharma, D. A. P., & Wiraguna, S. A. (2026). Analisis Hukum Dampak Kekosongan Lembaga Pengawas Pelindungan Data Pribadi Terhadap Petugas Pelindungan Data Di Indonesia. *Jurnal Kajian Ilmiah*, 26(1), 51–60. <https://doi.org/10.31599/3RTWFD20>
- Diantha, I. M. P. (2019). *Metodologi Penelitian Hukum Normatif Dalam Justifikasi Teori Hukum* (Cet. Ke-3). Prenadamedia group.
- Hernowo, B. A. (2025). The Challenges of Implementing the Personal Data Protection Law in Indonesia: Delays in Establishing a Regulatory Authority. *European Union Digital Library, Proceedings of the ... (ICL-C 2023)*, 1–12. <https://doi.org/10.4108/EAI.11-11-2023.2351333>
- Ibrahim, J. (2013). *Teori & Metodologi Penelitian Hukum Normatif*. Bayu Media Publishing.
- Irfandi. (2026). The Role of Law Enforcement in Upholding Privacy Regulations to Strengthen National Resilience in The Digital Era . *Multidisciplinary Indonesian Center Journal (MICJO)*, 3(1), 336–351. <https://doi.org/10.62567/MICJO.V3I1.1790>
- Joko Nursasih, M., & Sri Ratnaning Dhumillah, D. (2026). Personal Data Protection in Cases of Digital Breach (Criminal Law Review of Digital Platforms). *POSTULAT*, 4(1), 93–99. <https://doi.org/10.37010/POSTULAT.V4I1.2084>
- Khair, F., & Wiraguna, S. A. (2025). Data Protection Impact Assessment (DPIA) sebagai Instrumen Kunci Menjamin Kepatuhan UU PDP 2022 di Indonesia. *Politika Progresif: Jurnal Hukum, Politik Dan Humaniora*, 2(2), 246–254. <https://doi.org/10.62383/PROGRES.V2I2.1821>
- Kholik, I., Ediwarman, Ekaputra, M., & Mulyadi, M. (2024). Confiscation of Personal Assets of Corruption Defendants in a Positive Legal Perspective. *KnE Social Sciences*, 9(1), 359–373–359–373. <https://doi.org/10.18502/KSS.V8I21.14743>
- Kriswandar, A. S., Pratiwi, B., & Suwardi, S. (2024). Efektivitas Kebijakan Perlindungan Data Pribadi di Indonesia: Analisis Hukum Perdata dengan Pendekatan Studi Kasus. *Hakim: Jurnal Ilmu Hukum Dan Sosial*, 2(4), 740–756.

- <https://doi.org/10.51903/HAKIM.V2I4.2157>
- Lynskey, O. (2017). The 'Europeanisation' of Data Protection Law. *Cambridge Yearbook of European Legal Studies*, 19, 252–286. <https://doi.org/10.1017/CEL.2016.15>
- Marzuki, P. M. (2017). *Penelitian Hukum (Edisi Revisi)* (Cet. Ke-13). Pranadamedia Group.
- Nafisah, S., & Diniyanto, A. (2024). Independensi Lembaga Perlindungan Data Pribadi di Indonesia. *Manabia: Journal of Constitutional Law*, 4(01), 1–20. <https://doi.org/10.28918/MANABIA.V4I01.8664>
- Natamiharja, R. (2018). A Case Study on Facebook Data Theft in Indonesia. *Fiat Justisia: Jurnal Ilmu Hukum*, 12(3), 206–223. <https://doi.org/10.25041/FIATJUSTISIA.V12NO3.1312>
- Neta, Y., Awanisa, A., & Melisa, M. (2022). The Urgency of Establishing Independent Supervisory Authority for Personal Data Protection in Indonesia. *Constitutionale*, 3(1), 19–38. <https://doi.org/10.25041/CONSTITUTIONALE.V3I1.2535>
- Sholichah, M. P., & Rumaisa, D. (2018). Personal Data Protection Law Used in Mobile Phone Sim Card Registration in Indonesia. *Notaire*, 1(2), 269–284. <https://doi.org/10.20473/NTR.V1I2.9434>
- Siti Yuniarti, Ahmad M. Ramli, Sinta Dewi Rosadi, & Danrivanto Budhijanto. (2023). The New Chapter of Indonesia's Data Protection on Digital Economy Perspective. *Journal of Southwest Jiaotong University*, 58(3), 108–119. <https://doi.org/10.35741/ISSN.0258-2724.58.3.9>
- Soemitro, D. P., Wicaksono, M. A., & Putri, N. A. (2023). Penal Provisions in the Personal Data Protection Law: A Comparative Legal Study between Indonesia and Singapore. *SIGn Jurnal Hukum*, 5(1), 155–167. <https://doi.org/10.37276/SJH.V5I1.272>
- Suwondo, D. (2023). The Legal Protection of Personal Data in Islamic Perspective. *International Journal of Law Reconstruction*, 7(2), 221–230. <https://doi.org/10.26532/IJLR.V7I2.33648>
- Syafta, G., Fahni, R., & Ningsih, A. F. (2022). Independent Supervisory Authority to Protect Social Media Users' Personal Information in Indonesia. *Ius Poenale*, 3(1), 37–46. <https://doi.org/10.25041/IP.V3I1.2531>
- Syailendra, M. R., Lie, G., & Sudiro, A. (2024). Personal Data Protection Law in Indonesia: Challenges and Opportunities. *Indonesia Law Review*, 14(2), 56–72. <https://doi.org/https://doi.org/10.15742/ilrev.v14n2.4>
- Wachdin, S. Z. S., Adytia, N. A. P., & Said, S. (2024). The Legal Framework for Personal Data Protection in the Digital Era as Fulfillment of Privacy Rights in Indonesia. *KnE Social Sciences*, 9(1), 692–700–692–700. <https://doi.org/10.18502/KSS.V8I21.14785>
- Yuniarti, S. (2022). Protection of Indonesia's Personal Data After Ratification of Personal Data Protection Act. *Progressive Law Review*, 4(02), 54–68. <https://doi.org/10.36448/PLR.V4I02.85>