*Alauddin Law Development Journal (ALDEV)*
*Vol. 8, No. 1, 2026*

# URGENCY OF ESTABLISHING AN INDEPENDENT SUPERVISORY BODY TO IMPLEMENT ARTICLE 58 OF INDONESIA'S DATA PROTECTION LAW

**Muh. Arfhani Ichsan AH[1*], Muh. Chaerul Anwar[1]**
[1]Universitas Sulawesi Barat
*Correspondent Email: marfhaniichsan@unsulbar.ac.id

**Abstract**

*Digital transformation has increased the use of personal data along with the risks of data breaches and misuse. Indonesia has enacted Law Number 27 of 2022 concerning Personal Data Protection (PDP Law); however, its implementation remains ineffective due to the absence of a supervisory authority as mandated under Article 58 of the PDP Law. This study analyzes the impact of the absence of supervisory authority on the effectiveness of personal data protection and the obstacles to its establishment. This research employs a normative legal method and comparative approaches. The findings reveal that the absence of a supervisory authority results in weak oversight, low compliance among data controllers, and inadequate protection of data subjects' rights. Establishing an authority also faces institutional challenges, overlapping powers, limited resources, and low awareness of data protection culture. Therefore, an independent supervisory authority is urgently needed to strengthen the implementation of the PDP Law in Indonesia.*

*Keywords: Digital transformation; Personal data protection; Supervisory agency.*

**Abstrak**

Transformasi digital meningkatkan penggunaan data pribadi sekaligus resiko kebocoran dan penyalahgunaan data. Indonesia telah memiliki Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, namun implementasinya belum optimal karena belum terbentuknya lembaga pengawas sebagaimana diatur dalam Pasal 58 UU PDP. Penelitian ini menganalisis dampak kekosongan lembaga pengawas terhadap efektivitas perlindungan data pribadi serta kendala pembentukannya. Penelitian ini merupakan penelitian hukum normatif dan komparatif. Hasil penelitian menunjukkan bahwa ketiadaan lembaga pengawas menyebabkan lemahnya pengawasan, rendahnya kepatuhan pengendali data, serta tidak optimalnya perlindungan hak subjek data. Pembentukan lembaga pengawas juga menghadapi kendala kelembagaan, tumpang tindih kewenangan, keterbatasan sumber daya, dan rendahnya budaya perlindungan data. Oleh karena itu, diperlukan pembentukan lembaga pengawas independen untuk memperkuat implementasi UU PDP di Indonesia.

*Kata Kunci: Transformasi digital; Perlindungan data pribadi; Lembaga pengawas.*

DOI: 10.24252/aldev.v8i1.67700

*This is an open-access article under the CC BY-SA license.*

*Alauddin Law Development Journal (ALDEV)*
*Vol. 8, No. 1, 2026*

## INTRODUCTION

Digital transformation has brought fundamental changes in various aspects of people's lives, including in the management of personal data. The rapid development of information and communication technology has encouraged an increase in people's digital activities, such as the use of social media, electronic transactions, and services based on digital platforms. In today's era, the rate of internet penetration and the use of mobile devices is increasing. Internet-based applications, also known as over-the-top, have become an integral element of people's daily lives, including in Indonesia (Lia, 2018). In this context, personal data is no longer just individual information, but has evolved into a strategic asset that has high economic value. However, the increase in the use of this data is also followed by an increased risk of misuse and leakage of personal data (Bank, 2021). In recent years, Indonesia has faced various cases of personal data leaks that show the weakness of the data protection system. One of the major cases is the BPJS Kesehatan data leak involving more than 279 million Indonesian population data (Pangaribuan, 2024). This case shows that the data security system still has significant loopholes and has not been able to provide optimal protection to the community. In addition, various other data leak incidents continue to occur in the public and private sectors, which further emphasizes the urgency of personal data protection in Indonesia. Data that should be kept confidential is often traded on the dark web or misused for commercial purposes without the consent of the data subject. This phenomenon shows the weak legal protection system for consumer personal data in Indonesia, which in turn creates legal uncertainty and reduces public trust in electronic transactions (Fad, 2021).

The phenomenon of data leaks is also increasingly complex as the threat of cybercrime increases. Recent research shows that cyberattacks on personal data in Indonesia continue to increase and even target state institutions (Rendi, 2026). In Indonesia, we already have Law Number 27 of 2022 concerning Personal Data Protection, which is a big step to protect our personal data. However, its implementation still faces many challenges, one of the main challenges is the lack of public awareness about the importance of personal data protection, many of us do not yet understand how our personal data is collected, used, and shared by companies and government agencies (Suryanto & Riyanto, 2024). We need to conduct awareness and education campaigns on personal data protection, as well as improve the ability of law enforcement agencies to handle data leak cases (Erikha & Hoesein, 2025). This law is an important milestone in the national legal system because it provides comprehensive arrangements regarding the protection of personal data, including the rights of data subjects, the obligations of data controllers, as well as sanctions against breaches. However, the existence of regulations alone is not enough to guarantee the effectiveness of personal data protection.

Various studies show that the implementation of the Personal Data Protection Law still faces obstacles, especially in the aspect of supervision and law enforcement (Bachtiar, 2025).One of the main weaknesses is the lack of optimal formation of a personal data protection supervisory institution as mandated in Article 58 of the PDP Law. The absence of an independent supervisory institution has the potential to cause weak law enforcement and low levels of compliance with regulations. In addition, the protection of personal data is also closely related to human rights, especially the right to privacy. Research shows that personal data breaches not only impact economic losses, but can also threaten individual freedom (Rahmadani, 2025). Therefore, the state has an obligation to ensure effective protection systems, including through the establishment of strong supervisory institutions.

*Alauddin Law Development Journal (ALDEV)*
*Vol. 8, No. 1, 2026*

The existence of independent supervisory bodies has proven to be a key factor in the success of personal data protection. The European Union through the General Data Protection Regulation (GDPR) requires each member state to have an independent supervisory authority with broad powers in supervision and enforcement. This model has proven to be effective in improving compliance and providing more optimal protection of personal data. Studies show that in the absence of an independent supervisory body, data protection regulations tend to be ineffective in practice. This shows that the institutional aspect is a crucial element in the personal data protection system (Greenleaf, 2014). In the context of personal data, in developed countries, the term "privacy" is often used as a right that must be enforced, that is, the right of individuals to maintain their own life without interference (Latumahina, 2014). In today's era, the rate of internet penetration and the use of mobile devices is getting higher. Internet-based applications or also known as over the top have become an integral element of people's daily lives, including in Indonesia (Lia, 2018). From the perspective of legal theory, these failures can be analyzed using the legal system theory from Lawrence M. Friedman (1975), which states that the effectiveness of a legal system is determined by three elements, namely structure, substance, and culture. In the context of personal data protection in Indonesia, a legal substance (PDP Law) is available, but a legal structure in the form of a supervisory institution has not yet been formed. This structural vacuum causes the inability of the legal system to carry out the functions of supervision, enforcement, and legal protection optimally. In addition, the legal culture of the community and corporations that do not fully understand the importance of personal data protection is also a factor inhibiting the effective implementation of the PDP Law (Friedman, 1975).

In addition, the OECD also emphasized that countries with strong supervisory institutions tend to have higher levels of compliance and better public trust in digital systems. This shows that institutional aspects have a very important role in the personal data protection system (OECD, 2019).Therefore, in the context of the vacancy of supervisory institutions and the weak implementation of the PDP Law, structural legal reforms are needed. The reforms include accelerating the establishment of independent supervisory bodies, strengthening administrative supervision and sanction mechanisms, and developing a system for the protection of the rights of personal data subjects in digital transactions and e-commerce. Thus, personal data protection in Indonesia does not only stop at the normative level, but is actually implemented in practice through a legal system that is effective, responsive, and adaptive to the challenges of the times. Based on the above background, the author is interested in analyzing how the urgency of supervisory institutions in the Personal Data Protection Law (PDP) affects the effectiveness of personal data protection in Indonesia and the obstacles in the formation of supervisory institutions in the Personal Data Protection Law.

## METHOD

This research is normative legal research that examines legal materials related to the implementation of personal data protection, without collecting empirical data. The approach used includes an analysis of laws and regulations, especially Law Number 27 of 2022 concerning Personal Data Protection and its implementing regulations; tracing basic concepts of personal data, privacy, human rights, and information security; and a study of published cases of personal data violations. The data sources in this study consist of primary legal materials such as the PDP Law and ITE Law, as well as related government and ministerial regulations; secondary legal materials in the form of literature, scientific journals, and expert opinions; and tertiary legal materials such as legal dictionaries and encyclopedias that support the understanding of the legal material being studied.

*Alauddin Law Development Journal (ALDEV)*
*Vol. 8, No. 1, 2026*

## RESULT AND DISCUSSION

*1. The Impact of Supervisory Vacancy on Data Protection Effectiveness*

The absence of a personal data protection supervisory institution in Indonesia has significant legal consequences for the position of data protection officers. Normatively, Article 53 Paragraph (1) of the PDP Law has provided activity specifications that require data controllers and data processors to appoint data protection officers, especially in the context of processing personal data for public service activities, systematic monitoring of personal data on a large scale, and specific or related to criminal acts. Article 53, paragraph (2) of the PDP Law emphasizes that data protection officers must be appointed based on professionalism, legal knowledge, and ability to carry out their duties. Furthermore, in Article 53 Paragraph (3) of the PDP Law, it opens the possibility that data protection officers are parties who can be appointed both from inside and outside the controller and data processor(Rosadi, 2023) . However, this provision is not balanced by the existence of a supervisory authority that is authorized to verify whether the appointment of data protection officers has really been carried out and meets competency and independence standards (Faizah et al., 2023).

Legal reform refers to the process of changing or updating a legal system to be more in line with the times, societal needs, and challenges that arise in society. Legal reform not only includes changes in regulations, but also includes efforts to improve justice, efficiency, and legal certainty. This reform can be carried out through the revision of laws, the establishment of new regulations, or the reform of existing legal institutions. Legal reform aims to create a legal system that is more responsive to social, economic, and technological dynamics. This is especially relevant in the context of the rapid development of information technology and e-commerce, which demands better and more efficient protection of personal data (Soekanto, 2006). The legal theory put forward by Lawrence M. Friedman (1975) offers a relevant view in analyzing the legal system in the context of social change. Friedman argues that law is not a static entity, but an ever-evolving system, influenced by social, cultural, economic, and political factors. Friedman mentions three main elements in the legal system: the structure of the law, the substance of the law, and the culture of the law. The three are interconnected and must adapt to changes in society (Friedman, 1975).

In the context of the PDP Law, Friedman's theory emphasizes the importance of an efficient legal structure, which includes supervisory institutions that function to enforce regulations, as well as legal substance that suits the needs of society in the digital age. In addition, legal culture that includes people's attitudes towards the law and their rights also needs to be considered. Legal reforms in the context of the PDP Law should include changes in these three elements to create an effective personal data protection system. Law Number 27 of 2022 concerning Personal Data Protection (PDP Law) is an important regulation designed to protect the personal data of the Indonesian people. However, even though it has been passed, the implementation of the PDP Law still faces various challenges. One of the main problems is the absence of an independent supervisory institution, which is urgently needed to ensure that the implementation of the PDP Law runs well and in accordance with the principles of justice.

The absence of supervisory agencies results in the absence of an external oversight mechanism to ensure that the appointment of data protection officers is not just an administrative formality, but a tangible manifestation of the organization's commitment to responsible data governance. In practice, many companies that carry out massive data processing do not appoint data protection officers, on the grounds that their activities do not meet the mandatory criteria in Article 53 paragraph (1) of the PDP Law. Narrow interpretations of the phrases "large-scale" and "systematic monitoring" create structural legal loopholes that such entities exploit to avoid legal obligations, even though their activities clearly

*Alauddin Law Development Journal (ALDEV)*
*Vol. 8, No. 1, 2026*

fall within those criteria (Wiraguna, 2025). Law is always required to play its role in being able to anticipate all changes and developments that occur in society (Anwar et al., 2023). Regulations that are not updated regularly can result in policies that are outdated and irrelevant to the latest developments. For example, technologies such as AI, which can make decisions based on complex data, are often untouched by existing regulations (Smith, 2022).

Article 58 of the PDP Law states that the establishment of supervisory institutions is the responsibility of the government. However, in its realization, the institution has not yet been formed, causing a vacuum in supervision of data controllers and personal data processors. In fact, this institution is the most important part in providing supervision over the implementation of the rules. protection of personal data, as well as to take strict action against parties who violate consumer rights. Article 58 of the PDP Law states that "The Government establishes an institution that functions as a supervisor of data controllers and data processors responsible for the implementation of the provisions of this Law." The absence of this concrete supervisory institution worsens the effectiveness in the implementation of the PDP Law, because no party has the authority to actively supervise, reprimand, or sanction data controllers who violate existing provisions. Therefore, it is necessary to carry out clear legal reforms related to supervisory institutions and their authority (Nurhabibah et al., 2023). Although textually the provisions of the law have been improved, their application in the field still depends heavily on the understanding and interpretation of law enforcement officials. Without adequate implementation guidelines, the potential for abuse or disproportionate application of the law remains open (I.C.J.R., 2024).

In addition, the law does not provide a concrete legal protection mechanism in the implementation of its duties. As a result, data protection officers are in a vulnerable position, where they are operationally responsible but do not have full legal legitimacy to make strategic decisions if activities are found that risk privacy violations related to data protection policies in their environment. Moreover, without a supervisory institution, data protection officers do not have independent authorities that can be used as a reference in carrying out the duties of carrying out personal data protection functions. Such as consulting in providing information and advice on the assessment of the impact of personal data protection, monitoring and ensuring the performance of controllers and processors of personal data to comply with the provisions of the PDP Law, as well as coordinating and acting as a liaison person in resolving internal conflicts related to issues related to the processing of personal data, to reporting if there is a violation as per Article 54 Paragraph (1) of the PDP Law (Ajiraga, 2025).

Based on the need to improve the protection of personal data, several articles in the PDP Law need to be updated. One of the things that needs attention is Article 47 of the PDP Law, which regulates the responsibility of data controllers. This article is still too general and does not provide sufficiently specific details regarding the procedures that data controllers must carry out in managing personal data, as well as mechanisms to provide accountability in the event of data leaks. Article 47 of the PDP Law states "The data controller is responsible for the processing of personal data carried out and is obliged to ensure that the personal data is processed in accordance with the provisions of laws and regulations." However, this article should be amended to be more specific to discuss the sanctions received by data controllers who fail to protect personal data, as well as how consumers who are victims can get legal compensation or reparations. In addition, the PDP Law also needs to include clearer provisions on complaint procedures for consumers who are victims of data leaks. One potential legal consequence is the threat of accountability both administratively and through internal pressure on data protection officers. A weak legal structure allows data protection officers to be held accountable unilaterally. In fact, data management decisions are generally taken by the organization's management, not by data

*Alauddin Law Development Journal (ALDEV)*
*Vol. 8, No. 1, 2026*

protection officers. Without a supervisory agency that can objectively assess and distinguish administrative responsibilities from operational responsibilities, data protection officers are vulnerable to being scapegoated. This is clearly contrary to the principles of legal justice and the protection of policy implementers at the technical level(Karo & Prasetyo, 2020).

In the PDP Law, there is no guarantee that prohibits data controllers from giving instructions, dismissing, or imposing sanctions on data protection officers for carrying out their duties. This condition clouds the risk of conflict of interest, especially when data protection officers are appointed from within, such as legal staff or IT experts who are structurally dependent on management decisions. In addition, the absence of supervisory institutions hinders the development of professional standards and the capacity of data protection officers. In various jurisdictions that already have data protection authorities, the institution functions not only as a supervisor, but also as a training facilitator, issuer of technical guidance, as well as an intermediary in non-litigation disputes (Djafar et al., 2016). In Indonesia, data protection officers are forced to rely on personal interpretations or external sources that are not legally binding. This condition creates inconsistencies in the execution of tasks and increases the potential for procedural errors. This normative uncertainty can ultimately undermine the overall effectiveness of the personal data protection system that the state is supposed to guarantee (Pradhipta & Yudiantara, 2025).

However, without the existence of a personal data protection supervisory agency, the responsibilities of controllers and data processors as mandated in Articles 20–50 of the PDP Law become weak in implementation and lack effective enforcement mechanisms. This causes legal obligations that should be carried out concretely in practice only end up as declarative norms without guarantees of compliance and accountability. Normatively, data controllers are obliged to carry out compliance with the principles of fair, transparent, purpose-limited, and secure processing (Ginting & Ramadhan, 2025). However, the absence of supervisory authority creates a vacuum of legal space where the obligation does not have an external verification mechanism. As a result, many entities in both the public and private sectors only fulfill these obligations formally, for example by drafting privacy policies or Data Protection Impact Assessment (DPIA) documents without substantive implementation on the ground(Wardhono et al., 2024). In an effective data protection system, supervisory agencies play the role of external accountability guards that ensure data controllers not only declare compliance, but actually manifest it in practice. Without this institution, no entity is authorized to receive complaints, conduct investigations, examine data processing contracts between controllers and processors, and impose administrative sanctions as stipulated in Article 57 of the PDP Law. The PDP Law does regulate fines of up to IDR 4 billion or 2% of annual revenue, but these sanctions cannot be implemented without an authorized institution assessing and determining violations (Adhyputra et al., 2024). This condition weakens the deterrence and coercive power of legal norms, so that data controllers do not have a strong incentive to invest in good data governance, increasing the risk of privacy breaches.

The absence of a supervisory agency also blurs the boundaries of responsibility between controllers and data processors. Article 22 of the PDP Law requires data processors to act on the controller's instructions and implement adequate security measures (Theresa & Marlyna, 2024). However, in practice, this relationship is regulated through private contracts that are often not transparent to data subjects. Without a supervisor who can examine the content of the data processing contract or assess the proportionality of the division of responsibility, the risk of a breach is easily transferred unilaterally. For example, when a data leak occurs, controllers can blame the processor for "technical negligence," while the processor does not have an independent forum to defend itself or seek legal clarification(Martien, 2023).

Finally, without a supervisory agency, the rights of data subjects become collectively unenforceable. Although Article 43 of the PDP Law provides the right of access, correction, and deletion of data, dispute resolution mechanisms including mediation and complaint handling cannot operate without the competent authority (Chushairi et al., 2025). Data subjects are forced to file civil lawsuits individually, which is expensive, complicated, and disproportionate given the losses incurred. In fact, as affirmed in the Constitutional Court's ruling, the right to privacy is a constitutional right that must be effectively protected. Without a supervisory agency, the protection remains declarative, not operational. Thus, the responsibility of controllers and data processors in the absence of a supervisory agency becomes symbolic, immeasurable, and unenforceable. The PDP Act provides an adequate normative framework, but its institutional architecture is not complete. Without an independent, authoritative, and capable supervisory body, the entire personal data protection system risks collapsing into an administrative formality that is incapable of protecting the rights of citizens in the digital era full of data exploitation(G et al., 2025).

*2. Obstacles in the establishment of supervisory institutions in the Personal Data Protection Law*

The establishment of supervisory institutions as mandated in Article 58 of Law Number 27 of 2022 concerning Personal Data Protection is one of the most important elements in the implementation of the personal data protection system in Indonesia. The presence of supervisory institutions not only serves as an administrative instrument, but also as a key pillar in ensuring the effectiveness of law enforcement of personal data protection. In the context of the modern state of law, the existence of regulations without the support of strong supervisory institutions will cause the law to lose its implementing effectiveness. Therefore, the establishment of supervisory institutions in the PDP Law is an important part of realizing data protection governance that is accountable, transparent, and oriented towards human rights protection. However, the results of the study show that the establishment of a personal data protection supervisory institution in Indonesia still faces various multidimensional obstacles. These obstacles do not only come from normative aspects, but also include political and legal issues, institutional capacity, human resources, regulatory harmonization, and data protection culture in government systems and society. This condition shows that the implementation of Article 58 of the PDP Law is not fully ready to be carried out effectively.

One of the main obstacles in the formation of supervisory institutions is the lack of clarity in the institutional design regulated in the PDP Law. The law does mandate the existence of supervisory institutions, but does not provide detailed arrangements regarding the form, status, mechanism of appointment, institutional relations, or scope of authority. This ambiguity gives rise to various interpretations as to whether the supervisory agency will be established as an independent agency outside the ministerial structure or under a specific executive agency. From the perspective of state administrative law, the clarity of the institutional design is very important because it relates to the legitimacy, independence, and effectiveness of the exercise of an institution's authority. The unclear institutional construction has the potential to cause a conflict of authority and weaken the independence of the supervisory institution in the future. According to Christopher Kuner, the independence of supervisory institutions is a fundamental requirement in the modern data protection regime because the institution must be able to carry out supervision without political intervention or sectoral interests (Kuner, 2013). If the supervisory institution is under the direct control of the government, then there is a risk of a conflict of interest, especially when the data breach involves state institutions or public bodies.

*Alauddin Law Development Journal (ALDEV)*
*Vol. 8, No. 1, 2026*

In addition to the issue of institutional design, the formation of supervisory institutions also faces obstacles in the form of attracting interests and authority between state institutions. In the Indonesian government system, several institutions already have authority related to the supervision of electronic systems, cybersecurity, and digital information management. The Ministry of Communication and Information of the Republic of Indonesia, for example, has been carrying out a supervisory function for electronic system operators and digital infrastructure. On the other hand, there are also other institutions that have authority related to cybersecurity and data management in certain sectors. This condition leads to the emergence of sectoral egos and potential conflicts of authority in the formation of new supervisory institutions. The tug-of-war shows that the establishment of a personal data protection supervisory agency is not only related to legal needs, but also related to legal politics and the distribution of power in digital governance. In constitutional practice, the establishment of independent institutions often faces resistance from institutions that already have authority because they are considered to reduce the authority they have. As a result, the process of establishing a supervisory institution has been slow and lacks a clear direction.

From the perspective of institutional theory, the effectiveness of a regulation depends heavily on the capacity of its implementing institution. Colin J. Bennett and Charles D. Raab stated that the success of the data protection regime is greatly influenced by the state's ability to build independent, professional, and legitimately regulated regulatory institutions (Bennett & Raab, 2020). Therefore, without a supervisory institution that has clear authority and adequate capacity, the implementation of the PDP Law has the potential to be ineffective in practice. Another very important obstacle is the limitation of human resources and technological infrastructure. Personal data protection in the digital era requires high-tech surveillance involving digital audits, cyber forensic investigations, cross-electronic surveillance, and data risk analysis capabilities. However, Indonesia still faces a shortage of experts in the field of personal data protection and cybersecurity. This limitation is a serious obstacle in building supervisory institutions that are able to work professionally and adaptively to the development of digital technology.

In addition to human resources, the supervision technology infrastructure is also still relatively limited. In fact, modern supervisory institutions need a technological system that is able to quickly detect data breaches and conduct real-time supervision of personal data processing activities. Research in the Computer Law & Security Review shows that the effectiveness of data protection supervision is greatly influenced by the technological capacity and digital investigative capabilities of the supervisory agency(Franke, 2024). Without adequate technological support, supervisory institutions will find it difficult to carry out supervisory functions effectively. Another problem that is an obstacle is the fragmentation of personal data protection regulations in Indonesia. Prior to the birth of the PDP Law, regulations regarding personal data were spread across various sectoral regulations, such as regulations on telecommunications, health, banking, population administration, and electronic transactions. This condition causes data protection standards to develop partially and not integrate. This regulatory fragmentation also causes an overlap of authority between sectoral institutions. According to Lee A Bygrave, fragmented data protection systems tend to result in inconsistent law enforcement and undermine the effectiveness of data subject rights protection (Bygrave, 2014). When different sectors have different standards and supervisory mechanisms, legal certainty becomes difficult to achieve. In addition, coordination between institutions also becomes more complex because each institution has its own sectoral interests and regulations.

The next obstacle is the low data protection culture in Indonesia. Many institutions, both government and private, still view the protection of personal data as a purely administrative issue, not

*Alauddin Law Development Journal (ALDEV)*
*Vol. 8, No. 1, 2026*

as part of the protection of human rights and modern digital governance. This low awareness has led to the implementation of data protection principles, such as transparency, accountability, and data security, not yet being a top priority in the management of electronic systems. In the context of society, low digital literacy also causes people to not fully understand their rights as data subjects. As a result, many personal data breaches go unreported or do not receive serious attention. This condition shows that the formation of supervisory institutions is not enough only to be carried out through a normative approach, but must also be followed by the development of a data protection culture in society and state institutions. In a comparative perspective, countries that successfully implement data protection systems generally have independent supervisory institutions with broad authority and strong political support. The General Data Protection Regulation requires each EU member state to establish an independent supervisory authority that has the authority to investigate, audit, impose administrative sanctions, and resolve data protection disputes. This model has proven to be effective in increasing the level of compliance of data controllers and strengthening the protection of individual rights.

Graham Greenleaf stated that the existence of independent supervisory bodies is a key indicator of the success of data protection regimes in various countries (Greenleaf, 2014). Countries that have independent supervisory authorities tend to have higher levels of compliance and more effective data protection systems than countries that do not have such institutions. Thus, international experience shows that the existence of a supervisory institution is a fundamental necessity in a modern data protection system. It can be understood that the obstacles in the establishment of a personal data protection supervisory institution in Indonesia are complex and multidimensional. These obstacles include normative aspects, legal politics, institutions, human resource capacity, technological infrastructure, regulatory harmonization, and data protection culture. Therefore, strategic steps are needed in the form of regulatory harmonization, institutional capacity strengthening, increased data protection literacy, and strong political commitment so that the establishment of an independent supervisory institution can be realized effectively.

## CONCLUSION

The absence of a supervisory institution as mandated in Article 58 of Law Number 27 of 2022 concerning Personal Data Protection has an impact on the weak effectiveness of personal data protection in Indonesia. This institutional vacuum causes supervision of data controllers and processors to not run optimally, law enforcement is weak, and the protection of data subjects' rights has not been implemented optimally. In addition, the absence of a supervisory institution also creates legal uncertainty for the implementation of the duties of the Data Protection Officer. This study also found that the formation of supervisory institutions still faces various obstacles, such as unclear institutional design, overlapping authority between institutions, limited human resources and technology, and low data protection culture. In fact, based on international practice, the existence of an independent supervisory institution is an important element in creating an effective personal data protection system. Therefore, the government needs to immediately establish an independent, professional, and clear authority personal data protection supervisory institution so that the implementation of the PDP Law can run effectively and be able to ensure the protection of people's privacy rights in the digital era.

*Alauddin Law Development Journal (ALDEV)*
*Vol. 8, No. 1, 2026*

## REFERENCES

Adhyputra, M. F., Ahmadi, T., & Rifqi, M. (2024). Gagasan pelindungan data pribadi oleh LPPDP Indonesia: Sebuah studi perbandingan dengan otoritas pelindungan data pribadi Singapura. *Jurnal Nomokrasi: Jurnal Ledhak Fakultas Hukum UNHAS*, *2*, 56–74.

Ajiraga, H. (2025). *Peran dan tanggungjawab data protection officer dalam pelaksanaan perlindungan data pribadi*. *5*, 261–290.

Anwar, M. C., Fadhil, M. F., & Yasim, S. (2023). Implementasi budaya Malaqbiq dalam pencegahan tindak pidana kekerasan dalam rumah tangga di Kabupaten Majene. *Alauddin Law Development Journal*, *5*(3).

Bachtiar, F. R. (2025). Analisis penegakan hukum data pribadi. *Jurnal Amar*.

Bank, W. (2021). *World development report 2021: Data for better lives*. World Bank.

Bennett, C. J., & Raab, C. D. (2020). *The governance of privacy*. MIT Press.

Bygrave, L. A. (2014). *Data privacy law: An international perspective*. Oxford University Press.

Chushairi, S. M., Fithry, A., & Rusfandi. (2025). Perlindungan hukum bagi korban atas kebocoran pusat data nasional sementara (PDNs) perspektif perlindungan data pribadi. *Jendela Hukum*, *12*, 29–122.

Djafar, W., Sumigar, B. R. F., & Setianti, B. L. (2016). *Perlindungan data pribadi di Indonesia: Usulan pelembagaan kebijakan dari perspektif hak asasi manusia*. ELSAM.

Erikha, A., & Hoesein, Z. A. (2025). Strategi pencegahan kebocoran data pribadi: Peran Kominfo dan gerakan Siberkreasi dalam edukasi digital. *Jurnal Retentum*, *7*(1), 48–64.

Fad, M. F. (2021). Perlindungan data pribadi dalam perspektif Sadd Dzari'ah. *Muamalatuna*, *13*(1), 33–69.

Faizah, A. F., Dharmawan, A. F., Pratama, G. G., & Rosadi, S. D. (2023). Penguatan pelindungan data pribadi melalui otoritas pengawas di Indonesia berdasarkan perbandingan hukum Hong Kong dan Singapura. *Hakim: Jurnal Ilmu Hukum Dan Sosial*, *1*.

Franke, L. (2024). GDPR compliance and enforcement trends. *Computer Law & Security Review*.

Friedman, L. M. (1975). *The legal system: A social science perspective*. Russell Sage Foundation.

G, S. D., L, S. O. P., & K, A. K. P. (2025). *Urgensi pembentukan lembaga pengawas dalam pembaharuan hukum perlindungan data pribadi menurut Undang-Undang PDP*. *4*(2), 106–113.

Ginting, F. M., & Ramadhan, L. M. A. (2025). Urgensi pengesahan rancangan peraturan pemerintah tentang pelindungan data pribadi sebagai upaya mengatasi kesenjangan praktik terhadap kepatuhan. *LAKSMI SARI: Jurnal Pendidikan Dan Humaniora*, *4*, 1–12.

Greenleaf, G. (2014). *Asian data privacy laws*. Oxford University Press.

I.C.J.R. (2024). *Evaluasi Perubahan Kedua UU ITE dan Tantangan Implementasi (Policy Brief*.

Karo, R. P. K., & Prasetyo, T. (2020). *Pengaturan perlindungan data pribadi di Indonesia: Perspektif teori keadilan bermartabat*. Penerbit Nusa Media.

Kuner, C. (2013). *Transborder data flows and data privacy law*. Oxford University Press.

Latumahina, R. E. (2014). Aspek hukum perlindungan data pribadi di dunia maya. *Jurnal Gema Aktualita*, *3*(2), 17.

Lia, S. (2018). Urgensi Undang-Undang perlindungan data pribadi di Indonesia: Studi perbandingan hukum Inggris dan Malaysia. *Kanun Jurnal Ilmu Hukum*, *20*(2), 369–384.

Martien, D. (2023). *Perlindungan hukum data pribadi*. Mitra Ilmu.

Nurhabibah, N. I., Rosadi, S. D., & Nasution, F. U. (2023). Tanggung jawab pengendali data dalam memberikan pelindungan data pribadi anak di Indonesia: Studi komparasi negara Inggris. *MORALITY: Jurnal Ilmu Hukum*, *9*(2), 207–223.

OECD. (2019). *OECD privacy guidelines*. OECD Publishing.

Pangaribuan, L. M. P. (2024). Delik pencemaran nama baik dalam UU ITE: Kajian kritik dan perubahan. *Jurnal Hukum & Teknologi*, *5*(1), 13.

Pradhipta, A. P., & Yudiantara, I. G. N. K. (2025). *Analisis regulasi perlindungan data pribadi*. *3*(7).

Rahmadani, N. O. (2025). Data pribadi sebagai hak asasi manusia. *Jurnal PESHUM*.

Rendi, M. (2026). Perlindungan data pribadi dalam era digitalisasi. *Jurnal Hukum Lex Generalis*.

Rosadi, S. D. (2023). *Pembahasan UU pelindungan data pribadi (UU RI No. 27 Tahun 2022)*. Sinar Grafika.

Smith, J. (2022). Regulating digital innovation: Challenges and solutions. *Journal of Digital Regulation*, *12*(3), 123–145.

Soekanto, S. (2006). *Pengantar hukum Indonesia*. UI Press.

Suryanto, D., & Riyanto, S. (2024). Implementasi Undang-Undang Nomor 27 Tahun 2022 tentang perlindungan data pribadi dalam industri ritel: Tinjauan terhadap kepatuhan dan dampaknya pada konsumen. *VERITAS*, *10*(1), 121–135.

Theresa, G., & Marlyna, H. (2024). Pelindungan data pribadi pada layanan pendanaan berbasis teknologi informasi pasca Undang-Undang Nomor 27 Tahun 2022 dan Undang-Undang Nomor 4 Tahun 2023. *Jurnal Hukum & Pembangunan*, *54*(2). https://doi.org/10.21143/jhp.vol54.no2.1631

Wardhono, R. D. T. K., Badrawani, W., Deviana, A., Pramudyastuti, M., & Shalehanti, N. (2024). *Pelindungan data pribadi di Bank Indonesia dan lembaga jasa keuangan: Rekomendasi kebijakan dan teknis pengaturan* (Vol. 40).

Wiraguna, S. A. (2025). *Strengthening the functional autonomy of data protection officers under Indonesia's PDP Law 2022: A critical legal and institutional review*. *4*(3). https://doi.org/10.59818/jps.v4i3.2317