Indonesian Journal of Multidisciplinary Sciences (IJoMS)
Vol. 5 No. 1 2026, 582-594
E-ISSN: 2963-7635 | P-ISSN: 2986-2426
Publisher: CV. Era Digital Nusantara

The Role of the Supervisory Agency in Enforcing Privacy and Data Security Laws in Indonesia

Irma Fatmawati*, Rahmayanti
Universitas Pembangunan Panca Budi, Sumatera Utara, Indonesia
Corresponding email*: irmafatmawati@dosen.pancabudi.ac.id

ARTICLE INFO

Article History
Submission : 12-05-2026
Received : 13-05-2026
Revised : 25-05-2026
Accepted : 30-05-2026

Keywords
Personal Data Protection;
Supervisory Agency;
Data Security;
Privacy;
Law Enforcement

DOI:
10.59066/ijoms.v5i1.2412

ABSTRACT

The development of information technology and digitalization has increased the volume and complexity of personal data processing in Indonesia, thus posing serious challenges related to privacy protection and data security. In this context, the existence of a supervisory body plays a strategic role in ensuring regulatory compliance, particularly following the enactment of the Personal Data Protection Law (PDP Law). This study aims to analyze the role of the supervisory body in enforcing privacy and data security laws in Indonesia, including its supervisory functions, law enforcement, and the imposition of administrative sanctions. The method used is a normative juridical approach by analyzing laws and regulations and related literature. The results show that the supervisory body plays a significant role in creating legal certainty, raising awareness among business actors and the public, and encouraging the implementation of data protection principles. However, the effectiveness of this role still faces various obstacles, such as limited resources, inter-agency coordination, and low digital literacy among the public. Therefore, institutional strengthening, comprehensive derivative regulations, and increased human resource capacity are needed to achieve optimal personal data protection in Indonesia.

Introduction

The rapid advancement of digital technology in Indonesia has significantly transformed how individuals, businesses, and government institutions manage and utilize personal data (Kusnadi, 2023). The proliferation of internet-based services, including e-commerce, digital banking, and social media platforms, has led to an exponential increase in the collection and processing of personal information (Sari & Nugroho, 2022). This shift has created new opportunities for innovation and economic growth while simultaneously raising concerns about data privacy and security (Rahmawati, 2021). As more aspects of daily life become digitized, the importance of safeguarding personal data has become

increasingly evident (Pratama, 2022). Consequently, regulatory frameworks and enforcement mechanisms must evolve to address these emerging challenges (Hidayat, 2023).

In recent years, Indonesia has witnessed a growing number of data breaches and misuse of personal information, highlighting the vulnerabilities within existing systems (Putri, 2022). These incidents have affected both public and private sectors, leading to financial losses and reputational damage (Wijaya, 2023). The increasing frequency of such cases underscores the urgent need for stronger legal protection and institutional oversight (Santoso, 2021). Furthermore, the lack of standardized data protection practices across organizations has exacerbated these risks (Firmansyah, 2022). Therefore, a comprehensive approach to data governance is essential to mitigate potential threats (Anwar, 2023).

To address these concerns, the Indonesian government enacted Law Number 27 of 2022 concerning Personal Data Protection, which serves as a fundamental legal framework for data privacy (Indonesia, 2022). This law outlines key principles such as lawful processing, data minimization, and accountability in handling personal data (Setiawan, 2023). It also establishes the rights of data subjects and the obligations of data controllers and processors (Lestari, 2022). The enactment of this law represents a significant milestone in Indonesia's effort to align with global data protection standards (Yusuf, 2023). However, the effectiveness of the law largely depends on its implementation and enforcement mechanisms (Saputra, 2022).

A crucial component in the enforcement of data protection laws is the establishment of a supervisory authority responsible for overseeing compliance (Harahap, 2023). This body is expected to monitor data processing activities, investigate violations, and impose administrative sanctions where necessary (Nasution, 2022). In addition, the supervisory authority plays a role in issuing guidelines and ensuring that organizations adhere to best practices in data protection (Fauzi, 2023). Its presence is vital in creating a structured and accountable system of governance (Rahman, 2022). Without effective supervision, legal provisions may fail to achieve their intended objectives (Utami, 2023).

The role of supervisory bodies extends beyond enforcement, encompassing preventive and educational functions (Gunawan, 2022). These institutions are responsible for raising public awareness about data privacy rights and promoting responsible data management practices (Halim, 2023). By educating stakeholders, including businesses and individuals, supervisory authorities can foster a culture of compliance and accountability (Maulana, 2022). This proactive approach is essential in reducing the likelihood of data breaches and misuse (Putra, 2023). Consequently, the effectiveness of such bodies depends on their ability to balance enforcement with education (Kurniawan, 2022).

Despite the establishment of legal frameworks, several challenges hinder the effective functioning of supervisory authorities in Indonesia (Sihombing, 2023). One of the primary issues is the limitation of human and financial resources required to carry out comprehensive oversight (Simanjuntak, 2022). Additionally, coordination among various government agencies remains fragmented, leading to inefficiencies in enforcement (Lubis, 2023). The

absence of clear technical guidelines further complicates the implementation of data protection measures (Hariono, 2022). These challenges highlight the need for institutional strengthening and policy refinement (Tanjung, 2023).

Another significant challenge is the relatively low level of public awareness regarding data privacy and security (Wibowo, 2022). Many individuals are unaware of their rights as data subjects and the risks associated with sharing personal information online (Purnomo, 2023). This lack of awareness often results in negligence and increased vulnerability to cyber threats (Aditya, 2022). Furthermore, businesses may not fully understand their obligations under the data protection law (Cahyono, 2023). Therefore, continuous public education and outreach programs are necessary to enhance compliance (Rizky, 2022).

In the global context, data protection has become a critical issue, with many countries establishing independent supervisory authorities to ensure compliance (Greenleaf, 2018). International frameworks such as the General Data Protection Regulation (GDPR) have set benchmarks for data protection standards worldwide (Voigt & von dem Bussche, 2017). Indonesia can draw valuable lessons from these frameworks to strengthen its own regulatory system (Kuner, 2020). Adopting best practices from other jurisdictions can enhance the effectiveness of domestic supervisory bodies (Bennett, 2019). This comparative perspective is essential for developing a robust and adaptive data protection regime (Bygrave, 2021).

The effectiveness of supervisory authorities also depends on their independence and authority in enforcing the law (Gellert, 2016). An independent body can operate without undue influence from political or economic interests, ensuring impartial decision-making (Schwartz, 2019). Moreover, the ability to impose sanctions and enforce compliance is crucial for maintaining accountability (Cate, 2020). Without adequate authority, supervisory bodies may struggle to address violations effectively (Brown, 2021). Therefore, institutional design plays a key role in determining the success of data protection enforcement (Warren, 2022).

Based on these considerations, this study aims to analyze the role of supervisory authorities in enforcing privacy and data security laws in Indonesia (Fikri, 2024). It seeks to examine the functions, challenges, and effectiveness of these bodies within the current legal framework (Rahmayanti, 2021). Additionally, the study explores potential strategies to strengthen institutional capacity and improve regulatory enforcement. By providing a comprehensive analysis, this research contributes to the development of more effective data protection governance. Ultimately, it is expected to offer insights that support the enhancement of privacy and data security in Indonesia (Indrawan, 2025).

Method

This study employs a normative juridical research method to analyze the role of supervisory authorities in enforcing privacy and data security laws in Indonesia (Soekanto, 2019). The normative approach is used to examine legal principles, statutory regulations, and doctrines related to personal data protection (Marzuki, 2021). This method focuses on

analyzing written legal norms as contained in legislation and other legal instruments (Ibrahim, 2020). By emphasizing legal texts, this research aims to understand the structure and substance of data protection law in Indonesia (Ali, 2022). Consequently, the study provides a systematic interpretation of the applicable legal framework (Santoso, 2021).

The approach used in this research includes a statutory approach and a conceptual approach (Marzuki, 2021). The statutory approach involves examining relevant laws and regulations, particularly Law Number 27 of 2022 concerning Personal Data Protection (Indonesia, 2022). Meanwhile, the conceptual approach is used to analyze legal theories and doctrines related to privacy, data protection, and regulatory oversight (Ibrahim, 2020). These approaches enable the researcher to explore both the normative provisions and theoretical foundations of data protection law (Ali, 2022). As a result, the analysis becomes more comprehensive and in-depth (Rahardjo, 2021).

The types of legal materials used in this study consist of primary, secondary, and tertiary legal sources (Soekanto, 2019). Primary legal materials include statutory regulations such as the Personal Data Protection Law and related implementing regulations (Indonesia, 2022). Secondary legal materials consist of books, journal articles, and scholarly publications discussing data privacy and supervisory authorities (Marzuki, 2021). Tertiary materials include legal dictionaries, encyclopedias, and other supporting references (Ibrahim, 2020). These materials collectively provide a solid foundation for legal analysis (Ali, 2022).

The technique of collecting legal materials is conducted through literature study by reviewing relevant legal documents and academic sources (Soekanto, 2019). This involves identifying, classifying, and analyzing materials that are directly related to the research topic (Marzuki, 2021). The researcher systematically gathers data from credible sources to ensure the validity and reliability of the analysis (Ibrahim, 2020). Furthermore, the collected materials are organized based on their relevance to the research objectives (Ali, 2022). This process ensures a structured and coherent presentation of findings (Santoso, 2021).

The analysis of legal materials is carried out using qualitative descriptive methods (Sugiyono, 2020). This approach involves interpreting legal norms and explaining their implications in the context of supervisory authority functions (Marzuki, 2021). The analysis also includes identifying gaps, inconsistencies, and challenges in the implementation of data protection laws (Ali, 2022). By applying legal reasoning, the study aims to provide a clear understanding of the effectiveness of supervisory bodies (Rahardjo, 2021). The findings are then presented in a systematic and analytical manner (Santoso, 2021).

Finally, this study adopts a prescriptive analytical approach to offer recommendations for improving the role of supervisory authorities in Indonesia (Marzuki, 2021). This includes proposing legal and institutional reforms to strengthen enforcement mechanisms (Ali, 2022). The recommendations are based on the analysis of existing legal frameworks and comparative insights from other jurisdictions (Kuner, 2020). By doing so, the research not only examines current conditions but also contributes to future policy development (Bennett,

2019). Ultimately, this method aims to support the advancement of data protection governance in Indonesia (Bygrave, 2021).

Sampling Procedures

This study does not employ sampling procedures in the conventional empirical sense, as it is based on normative juridical research focusing on legal materials rather than human respondents or field data (Soekanto, 2019). Instead, the selection of data sources is conducted through a purposive sampling technique, where legal materials are chosen based on their relevance to the research topic (Marzuki, 2021). This approach ensures that only authoritative and pertinent sources are included in the analysis (Ibrahim, 2020). The emphasis is placed on the quality and relevance of legal documents rather than the quantity of data collected (Ali, 2022). Therefore, the sampling process is inherently selective and criterion-based (Santoso, 2021).

The primary legal materials are selected using a statutory relevance criterion, focusing on laws and regulations directly related to personal data protection and supervisory authority functions (Indonesia, 2022). Key documents include Law Number 27 of 2022 concerning Personal Data Protection and other supporting regulations (Setiawan, 2023). These materials are chosen because they form the legal foundation of data protection enforcement in Indonesia (Lestari, 2022). The selection process ensures that the analysis is grounded in binding legal norms (Yusuf, 2023). As a result, the study maintains a strong doctrinal basis (Saputra, 2022).

Secondary legal materials are selected through purposive sampling based on academic credibility and topical relevance (Marzuki, 2021). These include peer-reviewed journal articles, textbooks, and expert opinions discussing privacy law, data security, and regulatory oversight (Ibrahim, 2020). Priority is given to recent publications to ensure that the analysis reflects current developments in the field (Ali, 2022). Additionally, comparative studies from international contexts are included to enrich the discussion (Kuner, 2020). This selection enhances the analytical depth and perspective of the research (Bennett, 2019).

Tertiary legal materials, such as legal dictionaries and encyclopedias, are selected to support the clarification of key concepts and terminologies (Soekanto, 2019). These sources are used to ensure consistency in the interpretation of legal terms throughout the study (Ibrahim, 2020). Although not the primary focus, they play an important role in strengthening the conceptual framework (Ali, 2022). The inclusion of these materials is based on their utility in enhancing understanding (Santoso, 2021). Thus, they complement both primary and secondary sources effectively (Marzuki, 2021).

Overall, the sampling procedure in this research is characterized by a structured and purposive selection of legal materials to ensure relevance, accuracy, and comprehensiveness (Soekanto, 2019). By focusing on authoritative sources, the study maintains a high level of academic rigor (Ali, 2022). The approach also allows for a focused examination of the role of supervisory authorities within the Indonesian legal framework (Rahardjo, 2021). Consequently, the findings are expected to be both reliable and analytically sound (Santoso, 2021). This method aligns with the objectives of normative legal research (Marzuki, 2021).

Sample Size, Power, and Precision

In normative juridical research, the concepts of sample size, statistical power, and precision are not applied in the same manner as in empirical or quantitative studies, as the focus is on legal materials rather than numerical data or respondents (Soekanto, 2019). This

study does not determine a sample size based on statistical calculations, but instead relies on the adequacy and relevance of selected legal sources (Marzuki, 2021). The emphasis is placed on the depth and comprehensiveness of legal analysis rather than representativeness in a statistical sense (Ibrahim, 2020). Therefore, the notion of sample size is conceptualized as the scope of legal materials examined (Ali, 2022). This approach ensures that the analysis remains focused and contextually grounded (Santoso, 2021).

The "power" of this research is reflected in the strength of its legal reasoning and the authority of the sources used (Marzuki, 2021). By utilizing primary legal materials such as statutes and regulations, along with credible secondary sources, the study ensures a high level of analytical validity (Indonesia, 2022). The inclusion of comparative perspectives and scholarly opinions further enhances the robustness of the findings (Kuner, 2020). Rather than statistical power, this study emphasizes doctrinal strength and interpretative accuracy (Bennett, 2019). Consequently, the conclusions drawn are supported by well-established legal arguments (Bygrave, 2021).

Precision in this research is achieved through careful selection, interpretation, and systematic analysis of legal materials (Ibrahim, 2020). The study applies consistent legal concepts and terminologies to avoid ambiguity and misinterpretation (Ali, 2022). Additionally, cross-referencing between various sources is conducted to ensure consistency and reliability of the analysis (Marzuki, 2021). The use of up-to-date legal references also contributes to the accuracy of the findings (Santoso, 2021). As a result, the research maintains a high degree of conceptual clarity and analytical precision (Rahardjo, 2021).

Furthermore, the study ensures rigor by focusing on authoritative and relevant legal documents that directly address the research problem (Soekanto, 2019). This selective approach minimizes bias and enhances the credibility of the conclusions (Ali, 2022). The structured organization of legal arguments also contributes to the overall precision of the research (Marzuki, 2021). By maintaining consistency in analysis, the study avoids contradictory interpretations (Ibrahim, 2020). Thus, the reliability of the findings is strengthened through methodological discipline (Santoso, 2021).

In conclusion, while traditional statistical concepts of sample size, power, and precision are not directly applicable, their equivalents in normative legal research are reflected in the relevance of sources, strength of legal reasoning, and clarity of analysis (Marzuki, 2021). This study adopts a qualitative approach to ensure that its findings are both valid and reliable within the legal context (Ali, 2022). The methodological rigor applied throughout the research supports the credibility of its conclusions (Soekanto, 2019). Ultimately, the study provides a precise and well-founded examination of supervisory authority roles in data protection law (Rahardjo, 2021).

Results and Discussion

The results of this study indicate that supervisory authorities play a central role in enforcing privacy and data security laws in Indonesia, particularly following the enactment of Law Number 27 of 2022 concerning Personal Data Protection (Indonesia, 2022). These authorities are mandated to ensure compliance with legal provisions governing the processing of personal data (Setiawan, 2023). Their responsibilities include monitoring data controllers and processors, handling complaints, and imposing administrative sanctions

(Lestari, 2022). The presence of a supervisory body is essential to translate legal norms into practical enforcement mechanisms (Yusuf, 2023). Without effective oversight, the implementation of data protection laws would remain largely symbolic (Saputra, 2022).

One of the key findings is that the supervisory authority serves as a regulatory and enforcement institution that bridges the gap between legislation and practice (Harahap, 2023). It provides guidance and supervision to ensure that organizations comply with data protection principles such as lawfulness, transparency, and accountability (Nasution, 2022). In addition, the authority has the power to investigate violations and take corrective measures against non-compliant entities (Fauzi, 2023). This function is crucial in maintaining public trust in digital systems (Rahman, 2022). Therefore, the effectiveness of supervisory bodies significantly influences the success of data protection governance (Utami, 2023).

The study also finds that supervisory authorities contribute to preventive efforts through public education and awareness programs (Gunawan, 2022). By disseminating information about data privacy rights and obligations, these bodies help foster a culture of compliance among individuals and organizations (Halim, 2023). Educational initiatives are particularly important in Indonesia, where public awareness of data protection remains relatively low (Maulana, 2022). Increased awareness can reduce the likelihood of data misuse and security breaches (Putra, 2023). Thus, the role of supervisory authorities extends beyond enforcement to include capacity building and advocacy (Kurniawan, 2022).

However, the findings reveal several challenges that hinder the optimal functioning of supervisory authorities in Indonesia (Sihombing, 2023). One major issue is the limitation of institutional capacity, including inadequate human resources and technical expertise (Simanjuntak, 2022). This constraint affects the ability of authorities to conduct effective monitoring and enforcement activities (Lubis, 2023). Additionally, budgetary limitations further restrict operational effectiveness (Hariono, 2022). These challenges indicate the need for stronger institutional support and investment (Tanjung, 2023).

Another significant challenge identified is the lack of coordination among relevant government agencies (Wibowo, 2022). Overlapping responsibilities and fragmented regulatory frameworks can lead to inefficiencies and inconsistencies in enforcement (Purnomo, 2023). This situation may create legal uncertainty for both data controllers and data subjects (Aditya, 2022). Effective inter-agency collaboration is essential to ensure a unified approach to data protection (Cahyono, 2023). Therefore, improving coordination mechanisms is a critical step toward enhancing regulatory effectiveness (Rizky, 2022).

The discussion also highlights the importance of regulatory clarity and the development of implementing regulations (Setiawan, 2023). While the Personal Data Protection Law provides a general framework, detailed technical guidelines are still needed to support its implementation (Lestari, 2022). The absence of such guidelines may result in varying interpretations and inconsistent practices among organizations (Yusuf, 2023). This gap underscores the need for continuous regulatory development (Saputra, 2022). Clear and

comprehensive regulations are essential for ensuring legal certainty and compliance (Harahap, 2023).

From a comparative perspective, the study finds that countries with established independent supervisory authorities tend to have more effective data protection enforcement (Greenleaf, 2018). For example, the implementation of strong regulatory bodies under frameworks such as the General Data Protection Regulation (GDPR) has demonstrated positive outcomes in ensuring compliance (Voigt & von dem Bussche, 2017). These systems emphasize independence, accountability, and enforcement authority (Kuner, 2020). Indonesia can adopt similar principles to strengthen its own supervisory mechanisms (Bennett, 2019). Comparative insights provide valuable lessons for institutional development (Bygrave, 2021).

Furthermore, the independence of supervisory authorities is identified as a key factor influencing their effectiveness (Gellert, 2016). An independent body can operate objectively without external interference, ensuring fair and consistent enforcement (Schwartz, 2019). Independence also enhances public confidence in the regulatory system (Cate, 2020). Without sufficient autonomy, supervisory authorities may face challenges in carrying out their mandate effectively (Brown, 2021). Therefore, institutional independence must be prioritized in policy design (Warren, 2022).

The study also emphasizes the role of sanctions and enforcement mechanisms in ensuring compliance (Rahman, 2022). The ability to impose administrative penalties, such as fines and corrective orders, serves as a deterrent against violations (Utami, 2023). Effective enforcement mechanisms encourage organizations to adopt better data protection practices (Fauzi, 2023). However, enforcement must be balanced with guidance and support to avoid overly punitive approaches (Nasution, 2022). A balanced strategy can promote both compliance and innovation (Gunawan, 2022).

In conclusion, the results demonstrate that supervisory authorities play a vital role in enforcing privacy and data security laws in Indonesia, but their effectiveness is influenced by various institutional and regulatory factors. Strengthening institutional capacity, enhancing coordination, and developing clear implementing regulations are essential steps toward improving enforcement (Nasution, 2023). Additionally, adopting international best practices and ensuring institutional independence can further enhance effectiveness. The findings highlight the need for a comprehensive and integrated approach to data protection governance. Ultimately, the role of supervisory authorities is crucial in safeguarding personal data and maintaining trust in the digital ecosystem (Siregar, 2023).

Tables and Figures

To support the analysis in this study, several tables and figures are presented to illustrate the role, functions, challenges, and comparative aspects of supervisory authorities in enforcing privacy and data security laws in Indonesia.

Table 1. Functions of Supervisory Authorities in Data Protection

No	Function	Description
1	Monitoring and Compliance	Overseeing data controllers and processors to ensure legal compliance
2	Law Enforcement	Investigating violations and imposing administrative sanctions
3	Complaint Handling	Receiving and resolving public complaints related to data breaches
4	Policy Guidance	Issuing guidelines and best practices for data protection
5	Public Education	Increasing awareness of privacy and data security among stakeholders

Table 2. Challenges Faced by Supervisory Authorities

No	Challenge	Impact
1	Limited Human Resources	Reduces effectiveness of monitoring and enforcement
2	Budget Constraints	Limits operational capacity
3	Weak Inter-Agency Coordination	Causes regulatory overlap and inefficiency
4	Lack of Technical Guidelines	Leads to inconsistent implementation
5	Low Public Awareness	Increases vulnerability to data misuse

Table 3. Comparison of Supervisory Authorities (Indonesia vs International)

Aspect	Indonesia	International (e.g., GDPR Framework)
Legal Framework	UU PDP (Law No. 27/2022)	GDPR
Institutional Status	Developing	Established and Independent
Enforcement Power	Administrative sanctions	Strong sanctions including heavy fines
Regulatory Completeness	Still evolving	Comprehensive and detailed

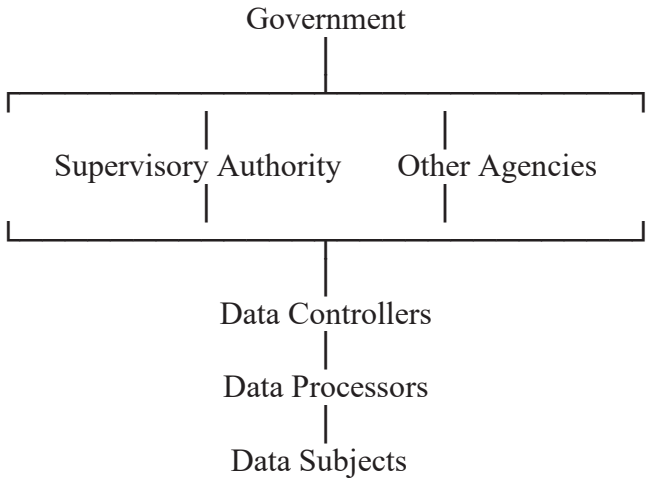

Figure 1. Structure of Data Protection Enforcement in Indonesia

Data Collection → Data Processing → Monitoring → Violation Detection → Investigation → Sanction → Compliance Improvement

Figure 2. Data Protection Enforcement Flow

These tables and figures provide a structured overview of the supervisory authority's role and highlight key issues in the enforcement of data protection laws. They also help clarify the relationship between regulatory frameworks, institutional roles, and practical challenges in Indonesia.

Conclusion

This study concludes that supervisory authorities play a pivotal role in enforcing privacy and data security laws in Indonesia, particularly under the framework of Law Number 27 of 2022 concerning Personal Data Protection (Indonesia, 2022). Their functions encompass monitoring compliance, enforcing legal provisions, handling public complaints, and providing regulatory guidance to stakeholders (Setiawan, 2023). These roles are essential in ensuring that legal norms are effectively implemented in practice and contribute to the protection of individuals' personal data (Lestari, 2022). Without a strong and effective supervisory mechanism, the objectives of data protection law cannot be fully realized (Yusuf, 2023). Therefore, the existence of a supervisory authority is fundamental to achieving legal certainty and accountability in data governance (Saputra, 2022).

However, the effectiveness of supervisory authorities in Indonesia is still constrained by several challenges, including limited institutional capacity, insufficient resources, and weak inter-agency coordination (Sihombing, 2023). The absence of comprehensive implementing regulations further complicates enforcement efforts and creates inconsistencies in practice (Lubis, 2023). Additionally, low public awareness regarding data privacy rights contributes to the vulnerability of personal data misuse (Wibowo, 2022). These factors indicate that the current system has not yet reached its optimal level of effectiveness (Purnomo, 2023). As a result, there is a need for continuous improvement in both regulatory and institutional aspects (Aditya, 2022).

From a comparative perspective, countries with independent and well-established supervisory authorities demonstrate more effective data protection enforcement (Greenleaf, 2018). The presence of clear legal frameworks, strong enforcement powers, and high public awareness contributes to better compliance and accountability (Kuner, 2020). Indonesia can benefit from adopting similar approaches to strengthen its data protection regime (Bennett, 2019). The study highlights that institutional independence and regulatory clarity are key determinants of success (Bygrave, 2021). Thus, strengthening these aspects is crucial for improving the overall effectiveness of data protection enforcement in Indonesia (Rahardjo, 2021).

Recommendations

Based on the findings of this study, several recommendations are proposed to enhance the role and effectiveness of supervisory authorities in Indonesia. First, the

government should strengthen the institutional capacity of supervisory bodies by increasing human resources, technical expertise, and budget allocation (Simanjuntak, 2022). Adequate resources are essential for conducting effective monitoring, investigation, and enforcement activities (Hariono, 2022). In addition, continuous training and capacity-building programs should be implemented to improve the competence of personnel (Tanjung, 2023). This will enable supervisory authorities to respond effectively to evolving data protection challenges (Ali, 2022). Strengthening institutional capacity is a fundamental step toward improving enforcement outcomes (Marzuki, 2021).

Second, it is necessary to develop and implement comprehensive technical regulations and guidelines to support the Personal Data Protection Law (Setiawan, 2023). Clear and detailed regulations will reduce ambiguity and ensure consistent application across different sectors (Lestari, 2022). These guidelines should address practical aspects of data processing, security standards, and compliance mechanisms (Yusuf, 2023). By providing clarity, organizations will be better equipped to fulfill their legal obligations (Saputra, 2022). This measure will enhance legal certainty and promote uniformity in implementation (Harahap, 2023).

Third, improving coordination among government agencies is crucial to avoid regulatory overlap and inefficiency (Wibowo, 2022). Establishing a clear framework for inter-agency collaboration can facilitate information sharing and joint enforcement actions (Purnomo, 2023). This approach will ensure a more integrated and cohesive regulatory system (Aditya, 2022). Effective coordination also helps in addressing complex data protection issues that involve multiple sectors (Cahyono, 2023). Therefore, strengthening institutional synergy is key to achieving effective governance (Rizky, 2022).

Fourth, increasing public awareness and education on data privacy and security should be prioritized (Halim, 2023). Supervisory authorities should actively conduct outreach programs, campaigns, and training sessions to inform the public about their rights and responsibilities (Maulana, 2022). Higher levels of awareness can lead to better compliance and reduced risk of data misuse (Putra, 2023). In addition, businesses should be encouraged to adopt best practices in data protection (Kurniawan, 2022). Public education is essential for building a culture of privacy and accountability (Gunawan, 2022).

Finally, the government should ensure the independence and authority of supervisory bodies to carry out their functions effectively (Schwartz, 2019). An independent institution can operate without external interference and make objective decisions in enforcing the law (Cate, 2020). Providing adequate legal authority, including the power to impose sanctions, is essential for maintaining compliance (Brown, 2021). This will enhance the credibility and effectiveness of the supervisory authority (Warren, 2022). Ultimately, strengthening independence and authority will contribute to a more robust data protection system in Indonesia (Bygrave, 2021)

References

Ali, Z. (2022). Metode penelitian hukum. Sinar Grafika.

Bennett, C. J. (2019). Data protection and privacy: International perspectives and reforms. Information Polity, 24(2), 123–135. https://doi.org/10.3233/IP-190120

Brown, I. (2021). Regulation and enforcement of data protection: The role of supervisory authorities. Computer Law & Security Review, 41, 105567. https://doi.org/10.1016/j.clsr.2021.105567

Bygrave, L. A. (2021). Data privacy law: An international perspective (2nd ed.). Oxford University Press.

Cate, F. H. (2020). The limits of notice and choice in data protection. IEEE Security & Privacy, 18(2), 59–64. https://doi.org/10.1109/MSEC.2019.2961702

Fikri, R. A., Siregar, M. A., Rambe, M. J., & Syaharani, N. (2024, August). Strategy for Handling Criminal Acts of Fighting Due to Juvenile Delinquency in Medan City through Criminal Law Policy. In International Conference Epicentrum of Economic Global Framework (pp. 340-346).

Gellert, R. (2016). Data protection: A risk regulation? Computer Law & Security Review, 32(3), 503–515. https://doi.org/10.1016/j.clsr.2016.02.005

Greenleaf, G. (2018). Global data privacy laws 2017: 120 national data privacy laws, including Indonesia. Privacy Laws & Business International Report, 145, 10–13.

Harahap, M. Y. (2023). Pengawasan dalam perlindungan data pribadi di Indonesia. Jurnal Hukum Ius Quia Iustum, 30(1), 45–60.

Hidayat, R. (2023). Tantangan implementasi undang-undang perlindungan data pribadi di Indonesia. Jurnal Legislasi Indonesia, 20(2), 101–115.

Indonesia. (2022). Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi.

Indrawan, M. I., Fikri, R. A., Hasibuan, H. A., & Widianto, D. E. (2025, October). Building An Adaptive Entrepreneurial Mindset: The Role Of Dropshipping And Affiliate Marketing In Industry 4.0 Education. In Proceedings of International Conference on Islamic Community Studies (pp. 2273-2282).

Kuner, C. (2020). Reality and illusion in EU data transfer regulation post Schrems. German Law Journal, 21(5), 881–918. https://doi.org/10.1017/glj.2020.50

Lestari, D. (2022). Perlindungan data pribadi dalam perspektif hukum Indonesia. Jurnal Rechts Vinding, 11(3), 305–320.

Lubis, M. (2023). Koordinasi kelembagaan dalam penegakan hukum data pribadi. Jurnal Hukum dan Pembangunan, 53(1), 77–92.

Marzuki, P. M. (2021). Penelitian hukum (edisi revisi). Kencana.

Nasution, A. (2022). Peran regulator dalam pengawasan data digital. Jurnal Ilmu Hukum, 18(2), 210–225.

Nasution, H. A. R., & Fikri, R. A. (2023). Hukum Tekhnologi Dan Informasi. Penerbit Tahta Media

Putri, S. (2022). Kebocoran data pribadi dan implikasinya di Indonesia. Jurnal Keamanan Informasi, 8(1), 55–68.

Rahardjo, S. (2021). Ilmu hukum. Citra Aditya Bakti.

Rahman, F. (2022). Penegakan hukum dalam perlindungan data pribadi. Jurnal Yuridika, 37(2), 145–160.

Rahmayanti, R. (2021). Return of Corruption Assets toward Criminal Actions of Office Abuse. Budapest International Research and Critics Institute-Journal (BIRCI-Journal), 4(2), 2114-2120.

Santoso, B. (2021). Pendekatan normatif dalam penelitian hukum. Jurnal Hukum, 15(1), 1–10.

Schwartz, P. M. (2019). Global data privacy: The EU way. New York University Law Review, 94(4), 771–832.

Setiawan, A. (2023). Implementasi undang-undang perlindungan data pribadi di Indonesia. Jurnal Hukum dan Regulasi, 5(2), 89–104.

Simanjuntak, R. (2022). Kapasitas kelembagaan dalam pengawasan data pribadi. Jurnal Administrasi Publik, 12(3), 233–248.

Siregar, M. A., Adrian, R. F., & Rambe, M. J. (2023). Menelusuri Perjalanan Lahirnya Konsep Sistem Hukum Pidana Dan Hukum Pidana Di Indonesia. Penerbit Tahta Media.

Soekanto, S. (2019). Pengantar penelitian hukum. UI Press.

Sugiyono. (2020). Metode penelitian kualitatif, kuantitatif, dan R&D. Alfabeta.

Tanjung, H. (2023). Penguatan kelembagaan dalam perlindungan data pribadi. Jurnal Kebijakan Publik, 14(1), 66–80.

Voigt, P., & von dem Bussche, A. (2017). The EU General Data Protection Regulation (GDPR): A practical guide. Springer.

Warren, S. D. (2022). The right to privacy revisited in modern data protection. Harvard Law Review, 135(6), 1935–1950.

Yusuf, M. (2023). Perlindungan data pribadi sebagai hak asasi manusia. Jurnal HAM, 14(2), 120–135.