IPSO JURE JOURNAL

IPSO JURE

Journal

E-ISSN : 3032-7644
https://nawalaeducation.com/index.php/IJJ/

Vol.2. No.4, May 2025
DOI : https://doi.org/10.62872/6p6kgm44

Digital Platforms' Responsibility for the Security of Users' Personal Data: A Juridical Analysis

Hendri Khuan[1], Saptaning Ruju Paminto[2], Nurul Fadhilah[3]
Universitas Borobudur, Indonesia[1], Universitas Suryakancana, Indonesia[2], Universitas Sriwijaya, Indonesia[3]

Received: March 15, 2025
Revised: April 17, 2025
Accepted: May 20, 2025
Published: May 30, 2025

Corresponding Author:
Author Name : Hendri Khuan
Email : hendri.khuan@gmail.com

Abstract: *The rapid development of information technology has created a complex and widespread digital ecosystem, where digital platforms are becoming massive collectors of personal data. This phenomenon poses a risk of data leakage and misuse that threatens individual privacy. In Indonesia, even though Law No. 27 of 2022 concerning Personal Data Protection (PDP Law) has been passed, its implementation still faces significant challenges, especially related to infrastructure readiness, law enforcement, and public awareness. Existing regulations tend to be normative and have not been able to keep up with rapid technological innovation, so the responsibility of digital platforms in maintaining data security is still weak and formalistic. This study uses a normative juridical approach to examine the effectiveness of the PDP Law in regulating the legal responsibilities of digital platforms. The results of the analysis show the need to strengthen supervision mechanisms, firm law enforcement, and increase technical capacity and human resources. Lessons learned from international standards emphasize the importance of independent oversight bodies and the application of privacy by design principles. With the synergy of adaptive regulations, reliable technology, and collective awareness, personal data protection can be realized effectively to protect users' rights and security in the digital era.*

Keywords: Juridical Analysis; Security-Personal Data; Responsibilities of Digital-Platforms

INTRODUCTION

The rapid growth of information and communication technology in the last two decades has led to the creation of a complex, dynamic, and expanding digital ecosystem into various sectors of life. Digital platforms such as social media, marketplaces, online transportation applications, application-based financial services, and e-government systems have become an integral part of modern society's life. In the process of their interaction, these platforms not only become a means of communication or transactions, but also become entities that massively collect and manage users' personal data, ranging from names,

Creative Commons Attribution-ShareAlike 4.0 International License:
https://creativecommons.org/licenses/by-sa/4.0/

IPSO JURE JOURNAL

IPSO JURE

Journal

E-ISSN : 3032-7644
https://nawalaeducation.com/index.php/IJJ/

Vol.2. No.4, May 2025
DOI : https://doi.org/10.62872/6p6kgm44

addresses, identity numbers, to behavioral preferences and biometric data.[1] This phenomenon has major consequences for the protection of personal data, as any digital activity has the potential to pose the risk of data leakage, misuse, or exploitation that is not in accordance with privacy principles. Many digital companies systematically monetize users' personal data without adequate transparency, which ultimately erodes an individual's sovereignty over his or her own data.[2]

This condition is exacerbated by the weak regulatory architecture and the lack of accountability from digital platforms in ensuring the security of personal data. In many countries, including Indonesia, personal data protection policies tend to lag behind the pace of technological innovation. Although Law No. 27 of 2022 concerning Personal Data Protection has been passed, its implementation still faces major challenges both in terms of infrastructure readiness, law enforcement, and public and corporate understanding of data protection obligations. The imbalance between the economic interests of digital platforms and the fundamental rights of users creates a significant power imbalance. Without strong legal controls and effective oversight mechanisms, digital platforms will continue to operate in the logic of data capitalism that ignores the ethics and privacy rights of users. Therefore, the growth of digital platforms must be accompanied by a critical analysis of legal responsibility structures and systemic efforts to strengthen the protection of personal data in the digital age.[3]

The vulnerability of personal data in the digital ecosystem is not just a technical issue, but reflects a structural failure to integrate security and privacy principles as a core part of digital system design (*privacy by design*). Many digital platforms prioritize user growth and monetization over the protection of the data they collect. This is reflected in the rampant incidents of data leaks that befall large institutions, both private and government. For example, the case of data leaks from BPJS Kesehatan in 2021 allegedly involving 279 million population data shows that the national cybersecurity infrastructure is not ready to deal with increasingly sophisticated attacks. According to reports, more than 80% of data breach incidents are caused by internal negligence and weak access controls.[4] This shows that the platform's responsibility is not only limited to reacting to incidents, but must involve ongoing and systematic preventive measures.

Furthermore, threats to the security of personal data are increasingly complex with the practice *of profiling* and *automated decision-making* based on artificial intelligence, which is often carried out without the explicit consent of the user. This situation creates an information imbalance between the data owner and

[1] Dwivedi, Y. K., Hughes, L., Baabdullah, A. M., Ribeiro-Navarrete, S., Giannakis, M., Al-Debei, M. M., ... & Wamba, S. F. (2022). Metaverse beyond the hype: Multidisciplinary perspectives on emerging challenges, opportunities, and agenda for research, practice and policy. *International journal of information management*, *66*, 102542.

[2] Manurung, E. A. P., & Thalib, E. F. (2022). Tinjauan yuridis perlindungan data pribadi berdasarkan UU nomor 27 tahun 2022. *Jurnal Hukum Saraswati*, *4*(2), 139-148.

[3] Daeng, Y., Linra, N., Darham, A., Handrianto, D., Sianturi, R. R., Martin, D., ... & Saputra, H. (2023). Perlindungan Data Pribadi dalam Era Digital: Tinjauan Terhadap Kerangka Hukum Perlindungan Privasi. *Innovative: Journal Of Social Science Research*, *3*(6), 2898-2905.

[4] Isnugraheny, R. F., Megawati, Z. E., & Susilawati, S. (2024). Optimalisasi Prinsip Kerahasiaan Data Nasabah dan Peranan Otoritas Jasa Keuangan Dalam Mencegah Kebocoran Informasi. *Media Hukum Indonesia (Mhi)*, *2*(4).

IPSO JURE JOURNAL

IPSO JURE

Journal

E-ISSN : 3032-7644
https://nawalaeducation.com/index.php/IJJ/

Vol.2. No.4, May 2025
DOI : https://doi.org/10.62872/6p6kgm44

the data controller, which in this case is a digital platform. As criticized by Shoshana Zuboff, the relationship between users and digital corporations has morphed into an invisible form of domination, where personal data is treated as a commodity without any commensurate protection. Ironically, existing regulations are often reactive and have not been able to keep pace with the pace of technological innovation.[5] The absence of the principles *of transparency, accountability,* and *consent* in the operational practices of digital platforms strengthens the position of users as vulnerable and helpless parties. Therefore, the urgency of personal data protection is not only a legal issue, but also an ethical and democratic issue that demands a deep and progressive reformulation of the legal responsibility of digital platforms.

The enactment of Law No. 27 of 2022 concerning Personal Data Protection (PDP Law) is a significant first step in answering the needs of regulation and legal certainty in the digital era. This law explicitly recognizes that personal data is part of the constitutionally guaranteed right to privacy and requires data controllers, including digital platforms, to implement protection principles such as transparency, validity of purpose, data minimization, and accountability. However, if you look deeper, this regulation is still normative and not fully adaptive to the complexity of rapidly changing digital technology practices. For example, the provisions regarding consent in data collection still rely heavily on formality without guaranteeing that users fully understand the risks or consequences of such consent. This indicates that the PDP Law still disproportionately places the burden of data protection on the data subject, not on the entity that controls and exploits the data.[6]

Furthermore, the fundamental weakness of the PDP Law is seen in its supervision and enforcement mechanisms. In Article 58, the government is indeed given the authority to establish a supervisory agency, but this institutional nature is not explicitly explained whether it is independent or under a specific ministry. This contrasts with an international approach that emphasizes the importance of structurally and functionally independent data protection authorities, as is the case with *the Data Protection Authority* in the GDPR. Without a strong independent institution free from political intervention or corporate interests, oversight of data breaches risks becoming symbolic and reactive. The PDP Law also does not regulate in detail the responsibility of digital platforms for new technologies such as artificial intelligence, big data, and algorithms that harbor discriminatory potential in data processing. Therefore, although the presence of the PDP Law is appreciative, critically, its substance and implementation are still far from sufficient to create a digital ecosystem that is fair, transparent, and in favor of the fundamental rights of users.[7]

Within the framework of juridical analysis, Law No. 27 of 2022 concerning Personal Data Protection (PDP Law) is the main legal instrument that regulates the responsibility of digital platforms for the security of users' personal data. The law classifies actors as "data controllers" and "data processors," each of which has

[5] Isnugraheny, R. F., Megawati, Z. E., & Susilawati, S. (2024). Optimalisasi Prinsip Kerahasiaan Data Nasabah dan Peranan Otoritas Jasa Keuangan Dalam Mencegah Kebocoran Informasi. *Media Hukum Indonesia (Mhi)*, *2*(4).

[6] Prayuti, Y. (2024). Dinamika perlindungan hukum konsumen di era digital: Analisis hukum terhadap praktik e-commerce dan perlindungan data konsumen di Indonesia. *Jurnal Interpretasi Hukum*, *5*(1), 903-913.

[77] Dhianty, R. (2022). Kebijakan Privasi (Privacy Policy) dan Peraturan Perundang-Undangan Sektoral Platform Digital vis a vis Kebocoran Data Pribadi. *Scripta: Jurnal Kebijakan Publik Dan Hukum*, *2*(1), 186-199.

IPSO JURE JOURNAL

IPSO JURE

Journal

E-ISSN : 3032-7644
https://nawalaeducation.com/index.php/IJJ/

Vol.2. No.4, May 2025
DOI : https://doi.org/10.62872/6p6kgm44

different responsibilities in the lifecycle of personal data, from data collection to destruction.[8] In Articles 35 to 50, the PDP Law regulates normatively the obligations of data controllers, including the need to implement adequate technical and organizational measures to prevent data leakage. However, from a critical perspective, the provisions tend to be generic and provide a wide range of interpretation without clear minimum standards. This creates potential *under-compliance* among digital platforms, especially large tech companies that have the capacity to lobby for regulations. As a result, the assessment of legal compliance tends to be formalistic and does not touch on the substance of the protection of user rights in a concrete way.

In addition, the effectiveness of the implementation and enforcement of sanctions in the PDP Law is still a big question mark. This law does contain provisions for administrative and criminal sanctions, such as fines, freezing of data processing activities, and the threat of imprisonment in certain cases. However, so far there is no legal precedent that shows that the sanctions are able to provide a deterrent effect on violators, especially large digital entities operating across jurisdictions. This shows weaknesses in the institutional design and law enforcement mechanisms of the PDP Law. Without a proactive monitoring system, independent investigations, and the role of the public and the media in overseeing the implementation of the law, the existence of sanctions will only become helpless articles. Therefore, the responsibility of digital platforms should be seen not only from formal compliance with the PDP Law, but also from the extent to which they substantially place the right to personal data protection as a fundamental principle in their technological operations and architecture.[9]

METHOD

examining primary and secondary legal materials as the basis for analysis. This approach is used to understand and review the legal norms that govern the responsibility of digital platforms in maintaining the security of users' personal data based on the framework of applicable laws and regulations.

The primary legal materials in this study include Law No. 27 of 2022 concerning Personal Data Protection (PDP Law), Law No. 11 of 2008 concerning Information and Electronic Transactions (ITE Law) and its amendments, as well as relevant implementing regulations. Secondary legal materials include legal literature, journal articles, previous research results, and the opinions of legal experts related to the protection of personal data and the responsibility of digital platforms. In addition, tertiary legal materials, such as legal dictionaries and legal encyclopedias, are also used to strengthen understanding of the concepts used.

The analysis technique used in this study is qualitative analysis, namely by interpreting the normative provisions in the PDP Law and related regulations to assess how the legal responsibility of digital platforms

[8] Wiraguna, S. A. (2025). Tanggung Jawab Hukum Platform E-Commerce atas Kebocoran Data Pribadi dalam Perspektif UU No. 27 Tahun 2022. *Jurnal Kajian Hukum Dan Kebijakan Publik| E-ISSN: 3031-8882*, *2*(2), 1089-1096.

[9] Mahameru, D. E., Nurhalizah, A., Badjeber, H., Wildan, A., & Rahmadia, H. (2023). Implementasi UU perlindungan data pribadi terhadap keamanan informasi identitas di Indonesia. *Jurnal Esensi Hukum*, *5*(2), 115-131.

IPSO JURE JOURNAL

IPSO JURE

Journal

Vol.2. No.4, May 2025
DOI : https://doi.org/10.62872/6p6kgm44

E-ISSN : 3032-7644
https://nawalaeducation.com/index.php/IJJ/

is regulated and the extent to which these provisions are able to provide effective legal protection to users. This research is also carried out in a prescriptive-analytical way, which not only describes the applicable legal norms, but also provides legal arguments and offers normative solutions to the weaknesses of the regulations found.

RESULTS AND DISCUSSION

Legal Responsibility of Digital Platforms as Data Controllers in the PDP Law

1. Analysis of Data Controllers' Obligations in the PDP Law: Principles of Data Protection and Security Systems

In the Personal Data Protection Law (PDP Law), the data controller in the context of a digital platform is the platform operator has legal obligations that are clearly regulated in Articles 35 to 50. This obligation includes the application of the basic principles of personal data protection that are the foundation of ethical and legal data management. One of the key principles is transparency, which requires data controllers to provide clear and easy-to-understand information to data owners about the purpose and manner in which their data is processed. This is important so that users are aware and can control their personal data. This principle is in line with the theory of the right to privacy which emphasizes the importance of individual control over personal information as the core of data protection.[10] Furthermore, the principle of lawfulness of the purposes of processing requires that the collection and use of data be based on legitimate grounds, such as the consent of the data owner or legal obligations. The principle of data minimization must also be adhered to, namely data controllers should only collect data that is really necessary for certain purposes to reduce the risk of misuse. This concept is supported by a study that develops the principle of Privacy by Design, which emphasizes reducing excessive data collection as a way to prevent privacy violations.[11] In addition, the data collected must be accurate, and its storage must not exceed the required time limits, in accordance with the principles of accuracy and storage restrictions in international standards such as GDPR.

In addition to the basic principles, the PDP Law also regulates the technical and organizational obligations for data controllers to maintain the security of personal data. Data controllers are required to implement security systems that include various measures such as data encryption to protect information when stored or transmitted, as well as access controls that limit only authorized parties from accessing the data. Regular supervision and audits are also an important part of detecting potential violations. No less important is the obligation to report data leakage incidents to the competent authorities and to the data owner within the specified time, so that transparency and risk mitigation can be carried out quickly. In this context, studies show that prompt and transparent reporting of incidents can reduce the negative impact of data leaks and

[10] Yel, M. B., & Nasution, M. K. (2022). Keamanan informasi data pribadi pada media sosial. *Jurnal Informatika Kaputama (JIK)*, *6*(1), 92-101.

[11] Alfitri, N. A., Rahmawati, R., & Firmansyah, F. (2024). Perlindungan terhadap data pribadi di era digital berdasarkan Undang-Undang Nomor 27 Tahun 2022. *Journal Social Society*, *4*(2), 92-111.

IPSO JURE JOURNAL

IPSO JURE

Journal

E-ISSN : 3032-7644
https://nawalaeducation.com/index.php/IJJ/

Vol.2. No.4, May 2025
DOI : https://doi.org/10.62872/6p6kgm44

increase public trust.[12] To support this, data controllers must ensure that all their staff and employees are adequately trained in data protection and security procedures.

Although the rules in Articles 35-50 of the PDP Law are quite comprehensive, their implementation in the field faces a number of challenges. Real threats such as cyberattacks that continue to grow, including hacking and ransomware, are one of the main risks that data controllers must anticipate. A study from the Verizon Data Breach Investigations Report (DBIR) shows an increasing trend of increasingly sophisticated cyberattacks, which demands an improvement also on the defense side of technology. In addition, the risk of data misuse from internal platform parties that is difficult to detect also requires data controllers to have strict control and supervision, which is supported by research that reveals that insider threats are one of the serious threats in data security[13]. No less important is readiness in terms of technology and human resources, especially for small digital business actors or startups that may not have an optimal data security system. Therefore, the effectiveness of the PDP Law is highly dependent on the seriousness of data controllers in implementing their technical and organizational obligations, as well as the active role of supervisory authorities in supervising and enforcing rules by providing strict sanctions for violations, as supported by the technology regulatory literature that highlights the importance of enforcement for legal effectiveness.[14]

Overall, the PDP Law provides a strong legal foundation for data controllers on digital platforms to carry out personal data protection responsibilities with clear principles and strict security obligations. However, to address real risks in an ever-evolving digital world, synergy between data controllers and regulators is needed, as well as continued investment in security technology and human resource training. Thus, personal data protection can be implemented effectively and provide a sense of security for users of the digital platform.

2. Comparison of Digital Platform Responsibilities in the PDP Law with International Standards: GDPR and Privacy by Design Principles

The Personal Data Protection Law (PDP Law) in Indonesia is a strategic response to the increasingly complex regulatory needs for personal data management in the digital era. This regulation seeks to adopt the main principles of international standards such as the European Union's General Data Protection Regulation (GDPR), especially in placing a huge responsibility on digital platforms in protecting user data. The accountability principles required in the GDPR require data managers to prove their compliance through complete documentation, regular audits, and the appointment of a Data Protection Officer (DPO) to ensure effective internal oversight. Accountability is a key pillar of the GDPR that forces organizations

[12] Isnugraheny, R. F., Megawati, Z. E., & Susilawati, S. (2024). Optimalisasi Prinsip Kerahasiaan Data Nasabah dan Peranan Otoritas Jasa Keuangan Dalam Mencegah Kebocoran Informasi. *Media Hukum Indonesia (Mhi)*, *2*(4).

[13] Adelika, A., & Nurbaiti, N. (2023). Upaya Pencegahan Terjadinya Pencurian Data Pada E-Ktp Bagi Penduduk Pada Dinas Kependudukan Dan Pencatatan Sipil Kota Medan. *Jurnal Pengabdian Masyarakat Khatulistiwa*, *6*(2), 124-133.

[14] Faizah, A. F., Rosadi, S. D., Pratama, G. G., & Dharmawan, A. F. (2023). Penguatan pelindungan data pribadi melalui otoritas pengawas di Indonesia berdasarkan perbandingan hukum Hong Kong dan Singapura. *Hakim: Jurnal Ilmu Hukum dan Sosial*, *1*(3), 01-27.

IPSO JURE JOURNAL

IPSO JURE

Journal

E-ISSN : 3032-7644
https://nawalaeducation.com/index.php/IJJ/

Vol.2. No.4, May 2025
DOI : https://doi.org/10.62872/6p6kgm44

to take full responsibility for data management, increasing transparency and public trust in digital platforms.[15] In the context of the PDP Law, this principle is also adopted, but according to the analysis, the regulation is still general and does not have a strong detailed mechanism like in the GDPR, so the implementation of accountability in Indonesia still needs to be strengthened in order to be able to answer the challenges of data breaches in the digital environment.[16]

In addition, the privacy by design principle in the GDPR is a proactive approach that integrates data protection from the early stages of system design. This principle encourages the application of encryption technology, data minimization, and strict access control to minimize the risk of data breaches. The originator of the concept of privacy by design, Cavoukian said that this approach not only improves data security but also fosters a culture of privacy protection within the organization. While the PDP Law has recognized the importance of this principle, regulations in Indonesia have not explicitly regulated its technical implementation, so its implementation is still highly dependent on the initiative of data managers. The absence of clear operational standards has the potential to undermine the effectiveness of data protection as a whole.

In terms of strength, the PDP Law has succeeded in harmonizing national regulations with international data protection principles, providing a strong legal basis for the protection of personal data. However, some weaknesses still emerge, especially related to the supervision and law enforcement mechanisms that are not optimal. As stated, effective data protection regulations must have an independent supervisory system and strict sanctions to have a deterrent effect.[17] This is still a challenge for the PDP Law. In addition, the role of data supervisors such as DPOs in the PDP Law has not been as open and clear as in the GDPR, which is a crucial element to ensure internal accountability and compliance of organizations.

Thus, although the PDP Law has laid the right foundation by adopting the principles of accountability and privacy by design, this regulation needs to be strengthened by adding technical provisions, audit mechanisms, and clear implementation standards in order to ensure the protection of users' rights as a whole. Synergy between regulations, technology, and privacy-oriented data management practices is key to facing data management challenges in the digital age.

Effectiveness of Law Enforcement and Supervision against Personal Data Security Violations

[15] Sidik, B. P., & Wiraguna, S. A. (2025). Tinjauan Hukum terhadap Aplikasi Digital sebagai Upaya Meningkatkan Kesadaran Perlindungan Hak Privasi Data Pribadi. *Hukum Inovatif: Jurnal Ilmu Hukum Sosial dan Humaniora*, *2*(2), 219-232.

[16] Rifa, F., & Hidayati, M. N. (2024). Kebijakan Penal dalam Perlindungan Data Pribadi Nasabah Fintech Lending di Indonesia. *Binamulia Hukum*, *13*(2), 461-481.

[17] Silalahi, J. A. S., Purba, Y. Y., & Nasution, M. F. (2025). Analisis Yuridis terhadap Mekanisme Perlindungan Data Pribadi dalam Sistem Informasi Elektronik Berdasarkan Perspektif Hukum Pidana di Indonesia. *Jurnal Minfo Polgan*, *14*(1), 604-613.

IPSO JURE JOURNAL

IPSO JURE

Journal

E-ISSN : 3032-7644
https://nawalaeducation.com/index.php/IJJ/

Vol.2. No.4, May 2025
DOI : https://doi.org/10.62872/6p6kgm44

1. Strengths and Weaknesses of Sanction Mechanisms in the PDP Law for Personal Data Security Violations

The Personal Data Protection Law (PDP Law) regulates various types of sanctions that can be imposed on perpetrators of personal data security violations, ranging from administrative sanctions such as financial fines, data processing freezes, to revocation of data processing permits, as well as criminal sanctions in the form of the threat of prison sentences for perpetrators of serious violations. This combination of sanctions reflects a comprehensive legal approach and aims to provide a strong deterrent effect. According to the theory of deterrence in criminology, the threat of a clear and unequivocal punishment can influence the behavior of individuals and organizations to obey the rules in order to avoid legal consequences.[18] Thus, the amount of fines and criminal threats in the PDP Law is expected to be a driver of compliance of data processing perpetrators.

Nevertheless, the effectiveness of these sanctions in practice faces a number of challenges. The study highlights that nationally enforced data protection regulations often face obstacles when applied to large tech companies operating across jurisdictions.[19] These multinational companies have complex legal resources and structures so that they are able to avoid national sanctions or minimize their impact. In addition, the long and complex legal process in the investigation of data breaches also often reduces the deterrent effect, the slow enforcement mechanism related to data privacy and security as a factor that weakens the effectiveness of regulations.

Furthermore, technical obstacles such as the lack of adequate digital evidence are also major challenges. Law enforcement against data breaches requires strong and digitally valid evidence, and the collection and verification of digital evidence requires specialized expertise and advanced technology that law enforcement officials in many countries, including Indonesia, have not yet equalized. Lack of coordination between agencies can also hinder the effectiveness of enforcement. According to the governance framework proposed by Heeks, synergy and collaboration between institutions are the main keys in managing complex and cross-sectoral data governance.

In addition, the awareness and capacity of business actors and law enforcement officials in understanding and implementing the PDP Law still need to be improved. According to the results of a survey by ENISA (European Union Agency for Cybersecurity, 2021), the level of understanding of data protection and technical capabilities in handling data security incidents greatly affect the successful implementation of data protection policies.

Therefore, although the PDP Law has regulated sanctions comprehensively and firmly, its implementation requires strengthening technical aspects and institutional coordination, as well as increasing cross-

[18] Isnawan, F. (2023). Pencegahan Tindak Pidana Kejahatan Jalanan Klitih Melalui Hukum Pidana dan Teori Kontrol Sosial. *Krtha Bhayangkara*, *17*(2), 349-378.

[19] Lase, I. N. (2024). Dampak Transformasi Digital terhadap Hukum Bisnis: Menghadapi Tantangan Hukum dalam Perdagangan Elektronik. *Jurnal Ilmu Hukum, Humaniora dan Politik (JIHHP)*, *5*(1).

IPSO JURE JOURNAL

IPSO JURE

Journal

E-ISSN : 3032-7644
https://nawalaeducation.com/index.php/IJJ/

Vol.2. No.4, May 2025
DOI : https://doi.org/10.62872/6p6kgm44

jurisdictional cooperation in order to provide a real deterrent effect, especially for large technology companies operating globally. Ongoing education and training for business actors and law enforcement officials are also an important part of supporting effective compliance and law enforcement. With the support of these measures, it is hoped that the sanctions mechanism in the PDP Law can provide optimal protection for the security of personal data in accordance with modern legal and information technology principles.

2. The Role and Challenges of Supervisory Institutions in Ensuring Digital Platform Accountability

Supervisory institutions play a crucial role in ensuring the accountability of digital platforms, especially in the context of personal data management. According to Article 58 of the Personal Data Protection Law (PDP), this institution is tasked with supervising the perpetrators of personal data management to comply with the principles of legal and transparent data protection. This is in line with the regulatory theory put forward by Majone (1997), which asserts that supervisory agencies must ensure that supervised entities are held accountable for their actions in the public interest. In addition to providing administrative sanctions, supervisory institutions also act as mediators for dispute resolution and drivers of public education. This function is important because research shows that the level of public awareness about data protection has a great effect on the effectiveness of data protection itself.[20]

However, the success of the supervisory institution is greatly influenced by its institutional status and independence. Indonesian law has not explicitly designated supervisory agencies as independent entities. This risks creating conflicts of interest and weakening the effectiveness of supervision. The independence of the supervisory institution is the main prerequisite for supervision to run without political and business pressure, which is in line with the principles of good governance.[21] In the context of data protection, this independence ensures that institutions can carry out their supervisory functions objectively. In addition, the capacity of human resources (HR) and technology is an important factor in the supervision of a highly dynamic digital platform. The importance of developing technological competencies and human resources who are able to understand the complexities of digital data management so that supervision is not only reactive, but also proactive.

Structural obstacles such as potential conflicts of interest are also serious challenges. Supervisory institutions that are not free from external influences tend to lose legitimacy and credibility in the eyes of the public. Plus, a lack of transparency in the oversight process will reduce institutional accountability, which is a key element for building public trust in supervisory institutions. In addition, low legal awareness

[20] Al Mustaqim, D., Hakim, F. A., Atfalina, H., & Fatakh, A. (2024). Peran media sosial sebagai sarana partisipasi warganet dalam mewujudukan keadilan dan akuntabilitas penegakan hukum di Indonesia. *Journal of Multidisciplinary Research and Development*, *1*(1), 53-66.

[21] Dewi, H. A. (2022). Independensi Aparat Pengawas Intern Pemerintah Guna Pelaksanaan Good Governance Berbasis CACM Di Lingkungan Pemerintah Daerah. *Arena Hukum*, *15*(2), 399-422.

IPSO JURE JOURNAL

IPSO JURE

Journal

E-ISSN : 3032-7644
https://nawalaeducation.com/index.php/IJJ/

Vol.2. No.4, May 2025
DOI : https://doi.org/10.62872/6p6kgm44

of users is another inhibiting factor. Active participation of users in data surveillance is indispensable to create a healthy digital ecosystem, as users who are aware of their rights can demand better protection.

In the international context, the surveillance model in Europe and some developed countries is an important reference. Data protection authorities such as the CNIL in France and the ICO in the UK which stand as independent bodies with full authority have shown effectiveness in overseeing and enforcing the protection of personal data. Transparency, technological capacity, and public engagement are key factors in their success. Meanwhile, models in Singapore and Australia that prioritize cross-sector collaboration have also been proven to be able to increase public legal awareness and the effectiveness of supervision. Based on the study, Indonesia needs to strengthen the institutional status of data supervisors to be more independent, increase the capacity of human resources and technology, and improve transparency and public participation mechanisms. Continuous education must also be a priority so that users' legal awareness increases and personal data protection can be carried out effectively in the ever-evolving digital era.

CONCLUSIONS

The Personal Data Protection Law (PDP Law) provides a strong legal basis for digital platforms as data controllers to carry out personal data protection responsibilities with clear basic principles, such as transparency, lawfulness of processing purposes, data minimization, and the obligation to maintain data security through strict technical and organizational systems. However, its implementation faces various real challenges, such as increasingly complex cyber threats, the risk of internal data misuse, and limited resources, especially for small business actors. When compared to international standards such as the GDPR, the PDP Law has adopted key principles such as accountability and privacy by design, but is still lacking in detailed technical, audit, and implementation mechanisms. Law enforcement against data breaches also still faces obstacles due to the complexity of the process, lack of adequate digital evidence, and coordination between agencies that is not optimal. Therefore, the effectiveness of the PDP Law is highly dependent on increased cooperation between data controllers and supervisory authorities, strengthening technical capacity and human resources, and continuous education for business actors and law enforcement officials. Supervisory institutions have a vital role in ensuring the accountability of digital platforms, but the institutional status that is not yet independent and the limited capacity of human resources and technology are the main challenges. Lessons from the international model show the need to strengthen independence, transparency, and public participation in data oversight. With the synergy between adaptive regulations, reliable technology, and privacy-oriented data management practices, personal data protection in the digital era can be implemented effectively and provide a sense of security for digital platform users.

REFERENCES

Adelika, A., & Nurbaiti, N. (2023). Upaya Pencegahan Terjadinya Pencurian Data Pada E-Ktp Bagi Penduduk Pada Dinas Kependudukan Dan Pencatatan Sipil Kota Medan. Jurnal Pengabdian Masyarakat Khatulistiwa, 6(2), 124-133.

IPSO JURE JOURNAL

IPSO JURE

Journal

E-ISSN : 3032-7644
https://nawalaeducation.com/index.php/IJJ/

Vol.2. No.4, May 2025
DOI : https://doi.org/10.62872/6p6kgm44

Al Mustaqim, D., Hakim, F. A., Atfalina, H., & Fatakh, A. (2024). Peran media sosial sebagai sarana partisipasi warganet dalam mewujudukan keadilan dan akuntabilitas penegakan hukum di Indonesia. Journal of Multidisciplinary Research and Development, 1(1), 53-66.

Alfitri, N. A., Rahmawati, R., & Firmansyah, F. (2024). Perlindungan terhadap data pribadi di era digital berdasarkan Undang-Undang Nomor 27 Tahun 2022. Journal Social Society, 4(2), 92-111.

Daeng, Y., Linra, N., Darham, A., Handrianto, D., Sianturi, R. R., Martin, D., ... & Saputra, H. (2023). Perlindungan Data Pribadi dalam Era Digital: Tinjauan Terhadap Kerangka Hukum Perlindungan Privasi. Innovative: Journal Of Social Science Research, 3(6), 2898-2905.

Dewi, H. A. (2022). Independensi Aparat Pengawas Intern Pemerintah Guna Pelaksanaan Good Governance Berbasis CACM Di Lingkungan Pemerintah Daerah. Arena Hukum, 15(2), 399-422..

Dhianty, R. (2022). Kebijakan Privasi (Privacy Policy) dan Peraturan Perundang-Undangan Sektoral Platform Digital vis a vis Kebocoran Data Pribadi. Scripta: Jurnal Kebijakan Publik Dan Hukum, 2(1), 186-199.

Dwivedi, Y. K., Hughes, L., Baabdullah, A. M., Ribeiro-Navarrete, S., Giannakis, M., Al-Debei, M. M., ... & Wamba, S. F. (2022). Metaverse beyond the hype: Multidisciplinary perspectives on emerging challenges, opportunities, and agenda for research, practice and policy. International journal of information management, 66, 102542.

Faizah, A. F., Rosadi, S. D., Pratama, G. G., & Dharmawan, A. F. (2023). Penguatan pelindungan data pribadi melalui otoritas pengawas di Indonesia berdasarkan perbandingan hukum Hong Kong dan Singapura. Hakim: Jurnal Ilmu Hukum dan Sosial, 1(3), 01-27.

Isnawan, F. (2023). Pencegahan Tindak Pidana Kejahatan Jalanan Klitih Melalui Hukum Pidana dan Teori Kontrol Sosial. Krtha Bhayangkara, 17(2), 349-378.

Isnugraheny, R. F., Megawati, Z. E., & Susilawati, S. (2024). Optimalisasi Prinsip Kerahasiaan Data Nasabah dan Peranan Otoritas Jasa Keuangan Dalam Mencegah Kebocoran Informasi. Media Hukum Indonesia (Mhi), 2(4).

Isnugraheny, R. F., Megawati, Z. E., & Susilawati, S. (2024). Optimalisasi Prinsip Kerahasiaan Data Nasabah dan Peranan Otoritas Jasa Keuangan Dalam Mencegah Kebocoran Informasi. Media Hukum Indonesia (Mhi), 2(4).

Isnugraheny, R. F., Megawati, Z. E., & Susilawati, S. (2024). Optimalisasi Prinsip Kerahasiaan Data Nasabah dan Peranan Otoritas Jasa Keuangan Dalam Mencegah Kebocoran Informasi. Media Hukum Indonesia (Mhi), 2(4).

Lase, I. N. (2024). Dampak Transformasi Digital terhadap Hukum Bisnis: Menghadapi Tantangan Hukum dalam Perdagangan Elektronik. Jurnal Ilmu Hukum, Humaniora dan Politik (JIHHP), 5(1).

IPSO JURE JOURNAL

IPSO JURE

Journal

Vol.2. No.4, May 2025
DOI : https://doi.org/10.62872/6p6kgm44

E-ISSN : 3032-7644
https://nawalaeducation.com/index.php/IJJ/

Mahameru, D. E., Nurhalizah, A., Badjeber, H., Wildan, A., & Rahmadia, H. (2023). Implementasi UU perlindungan data pribadi terhadap keamanan informasi identitas di Indonesia. Jurnal Esensi Hukum, 5(2), 115-131.

Manurung, E. A. P., & Thalib, E. F. (2022). Tinjauan yuridis perlindungan data pribadi berdasarkan UU nomor 27 tahun 2022. Jurnal Hukum Saraswati, 4(2), 139-148.

Prayuti, Y. (2024). Dinamika perlindungan hukum konsumen di era digital: Analisis hukum terhadap praktik e-commerce dan perlindungan data konsumen di Indonesia. Jurnal Interpretasi Hukum, 5(1), 903-913.

Rifa, F., & Hidayati, M. N. (2024). Kebijakan Penal dalam Perlindungan Data Pribadi Nasabah Fintech Lending di Indonesia. Binamulia Hukum, 13(2), 461-481.

Sidik, B. P., & Wiraguna, S. A. (2025). Tinjauan Hukum terhadap Aplikasi Digital sebagai Upaya Meningkatkan Kesadaran Perlindungan Hak Privasi Data Pribadi. Hukum Inovatif: Jurnal Ilmu Hukum Sosial dan Humaniora, 2(2), 219-232.

Silalahi, J. A. S., Purba, Y. Y., & Nasution, M. F. (2025). Analisis Yuridis terhadap Mekanisme Perlindungan Data Pribadi dalam Sistem Informasi Elektronik Berdasarkan Perspektif Hukum Pidana di Indonesia. Jurnal Minfo Polgan, 14(1), 604-613.

Wiraguna, S. A. (2025). Tanggung Jawab Hukum Platform E-Commerce atas Kebocoran Data Pribadi dalam Perspektif UU No. 27 Tahun 2022. Jurnal Kajian Hukum Dan Kebijakan Publik| E-ISSN: 3031-8882, 2(2), 1089-1096.

Yel, M. B., & Nasution, M. K. (2022). Keamanan informasi data pribadi pada media sosial. Jurnal Informatika Kaputama (JIK), 6(1), 92-101.