International Journal of Business, Law, and Education
Publisher: IJBLE Scientific Publications Community Inc.
Volume 6, Number 2, 2025
https://ijble.com/index.php/journal/index

The Legal Protection of Personal Data in the Digital Era: A Comparative Study of Indonesian Law and the GDPR

Muchamad Taufiq[1], Mochamad Reza Kurniawan[2], Ananda Salsabila Kenyo[3]
ITB Widya Gama Lumajang[1,2,3]
muchamadtaufiq1009@gmail.com[1], mochamadrezakurniawan@gmail.com[2], anandakenyo@gmail.com[3]

ABSTRACT
In the rapidly evolving digital era, personal data has emerged as a valuable asset, necessitating comprehensive legal frameworks to ensure privacy and security. This study aims to compare the legal protection of personal data under Indonesia's Personal Data Protection Law (UU No. 27/2022) with the European Union's General Data Protection Regulation (GDPR). Utilizing a normative legal research method and comparative approach, this research analyzes core principles, data subject rights, the obligations of data controllers and processors, as well as supervisory and enforcement mechanisms in both legal systems. The findings reveal that while the Indonesian PDP Law shares several foundational elements with the GDPR it remains less developed in terms of procedural detail, institutional readiness, and enforceability. The GDPR offers a more mature and integrated approach, featuring robust data subject rights, mandatory Data Protection Impact Assessments (DPIAs), independent supervisory authorities, and extraterritorial applicability. To align with international best practices and adequately protect citizens' digital rights, Indonesia must enhance the implementation of its PDP Law through clearer regulations, stronger enforcement institutions, and broader public awareness. This comparative analysis contributes to the academic discourse on data protection and offers practical insights for policymakers and legal practitioners in emerging digital economies.

Keywords:
Personal Data Protection; GDPR; Indonesia PDP Law; Digital Privasy; Data Subject Rights

INTRODUCTION

In the digital era, personal data has become a highly valuable asset, often referred to as the "new oil" of the 21st century. The exponential growth of digital platforms such as social media, e-commerce, mobile applications, and cloud computing has led to massive data collection, processing, and analysis activities. These developments have elevated the urgency for robust personal data protection mechanisms to ensure that individuals' rights to privacy are not undermined. As data flows seamlessly across borders, ensuring adequate legal protection for personal data becomes increasingly complex and requires not only national but also international legal frameworks (Greenleaf, 2012).

The issue of personal data protection has gained traction globally, especially due to several high-profile data breaches and misuse of personal information. Incidents such as the Cambridge Analytica scandal, which involved the misuse of data from millions of Facebook users, have highlighted the potential dangers when personal data is inadequately protected (Isaak & Hanna, 2018). In response, the European Union (EU) implemented the General Data Protection Regulation (GDPR) in 2018, which is now considered the global benchmark for data protection legislation. The GDPR enforces strict consent requirements, data subject rights, and accountability principles, influencing data privacy laws in numerous other jurisdictions (Voigt & Von dem Bussche, 2017).

Indonesia, as the largest digital economy in Southeast Asia, faces pressing challenges in protecting personal data. The growth of internet users in Indonesia, which exceeded 210 million in 2023 (APJII, 2023), reflects a high volume of digital transactions and interactions that inherently involve personal data exchange. However, until recently, Indonesia did not have a specific and comprehensive data protection law. While certain provisions related to privacy were embedded in sectoral regulations and the Electronic Information and Transactions Law (UU ITE No. 11/2008), these frameworks lacked clarity, consistency, and enforcement capacity (Setiadi, 2020). Recognizing this gap, the Indonesian government finally enacted the Personal Data Protection Law (UU PDP No. 27/2022), signaling a critical step toward strengthening data privacy governance.

Despite this development, the new Indonesian PDP Law still raises questions regarding its alignment with international standards, especially the GDPR. While there are similarities in terms of the general principles such as consent, transparency, and data minimization, differences remain in regulatory approaches, scope of protection, enforcement mechanisms, and the role of supervisory authorities (Ghozali, 2022). For instance, the GDPR's emphasis on extraterritorial applicability, the “right to be forgotten,” and data protection impact assessments is more far-reaching compared to its Indonesian counterpart. This raises important questions about whether the Indonesian PDP Law is adequate in addressing current and future data protection challenges in the global digital ecosystem.

The comparative study between the Indonesian legal framework and the GDPR is not merely academic; it has significant practical and policy implications. As Indonesia deepens its engagement with the digital economy and global data flows, harmonization with international norms becomes increasingly crucial. Businesses, particularly those engaging in cross-border transactions or servicing European users, must ensure compliance not only with domestic laws but also with foreign regulations such as the GDPR. At the same time, individuals need assurance that their digital rights are respected and protected regardless of where their data is processed.

Given the rapid development of digital technologies and the increasing risks to personal data security, Indonesia has taken important steps by enacting the Personal Data Protection Law in 2022. However, questions remain regarding the comprehensiveness, effectiveness, and enforcement of this law in comparison with internationally recognized standards such as the European Union’s General Data Protection Regulation (GDPR). There is a gap in academic literature and policy discourse that critically evaluates the extent to which the Indonesian legal framework aligns with the GDPR in providing effective legal protection of personal data. This study addresses the problem of whether Indonesia’s legal provisions on personal data protection offer an adequate legal framework to safeguard individual rights in the digital era, and how these provisions compare to the GDPR in terms of scope, principles, and enforcement mechanisms. This study aims to conduct a comparative legal analysis of Indonesia’s Personal Data Protection Law (UU PDP No. 27/2022) and the European Union’s General Data Protection Regulation (GDPR) to evaluate the effectiveness of legal protections for personal data in the digital era.

METHOD

This study employs a normative legal research method with a comparative approach. Normative legal research focuses on analyzing legal norms, principles, and statutory provisions by using legal materials such as legislation, case law, legal doctrines, and scholarly writings (Soekanto & Mamudji, 2004). The main sources of data in this study are primary legal materials, including Indonesia's Personal Data Protection Law (UU No. 27/2022) and the European Union's General Data Protection Regulation (GDPR). Secondary legal materials such as legal commentaries, journal articles, policy papers, and academic books are also reviewed to provide contextual understanding and doctrinal interpretation. The comparative analysis is conducted to identify similarities and differences between the two legal systems in terms of data protection principles, rights of data subjects, obligations of data controllers, enforcement mechanisms, and cross-border data transfer regulations. The study also uses a qualitative content analysis technique to interpret legal texts in light of international best practices and evolving digital privacy challenges..

RESULTS AND DISCUSSION

1. General Principles of Personal Data Protection: Alignment and Divergence

The Indonesian Personal Data Protection Law (Undang-Undang No. 27 Tahun 2022 tentang Perlindungan Data Pribadi, hereinafter referred to as "UU PDP") and the European Union's General Data Protection Regulation (GDPR) both reflect a shared commitment to safeguarding personal data in the era of digital transformation. These two regulatory frameworks are built on a similar foundation of fundamental principles intended to ensure that personal data is processed fairly, lawfully, and transparently. Both legal regimes recognize and codify key principles, including lawfulness, fairness, transparency, purpose limitation, data minimization, accuracy, storage limitation, integrity and confidentiality, and accountability. These principles serve as normative guidelines for all data processing activities, helping to strike a balance between data innovation and individual privacy rights.

For example, Article 4 of the Indonesian PDP Law lays down several core principles of data protection that mirror those found in Article 5 of the GDPR. Both regulations emphasize that data must be collected for specific, explicit, and legitimate purposes and not further processed in a manner incompatible with those purposes. Additionally, both require that personal data be accurate and kept up to date, and that data must be stored only as long as necessary for the purposes for which it was collected. The principle of integrity and confidentiality is also enshrined, obligating data controllers to implement appropriate technical and organizational measures to protect personal data from unauthorized access, loss, or destruction.

However, despite these similarities, a more detailed examination reveals substantive divergences in the formulation, depth, and enforceability of these principles between the two jurisdictions. The GDPR is notably more comprehensive and operationalized in both scope and application. One significant example is the GDPR’s expanded legal basis for data processing under Article 6, which outlines six specific bases: consent, contractual necessity, legal obligation, protection of vital interests, performance of a task carried out in the public interest or in the exercise of official authority, and legitimate interests pursued by the data controller or a third party.

This provides organizations with greater flexibility while still ensuring strong protection for data subjects.

In contrast, the Indonesian PDP Law places overriding emphasis on consent as the primary and, in most cases, the sole legal basis for data processing (UU PDP, Articles 20–22). While consent is a cornerstone of data protection law, relying on it exclusively may prove insufficient in complex or large-scale data environments. This narrow framework may constrain both public and private sector entities from efficiently processing personal data for lawful purposes where obtaining explicit consent may not be practical or necessary such as fraud prevention, internal auditing, or public safety measures. The lack of diverse legal bases can create legal uncertainty and operational limitations for data controllers.

Another notable divergence is the principle of data protection by design and by default, which is a hallmark of the GDPR (Art. 25). This principle requires that data protection measures be integrated into the development of business processes, technologies, and products from the outset (privacy by design), and that only data necessary for a specific purpose be processed (privacy by default). This proactive and preventive approach obligates organizations to assess risks and implement safeguards during the entire data lifecycle. The GDPR requires documentation, regular reviews, and the incorporation of data minimization into technological systems.

Indonesia's PDP Law lacks a direct equivalent to this principle. Although the Indonesian law does require data controllers to ensure the security and protection of personal data through appropriate technical and organizational measures (UU PDP Article 39), the proactive and embedded design orientation of the GDPR is not reflected in the Indonesian legal framework. As a result, there is a potential risk that data protection in Indonesia may be approached reactively, addressing risks only after breaches or incidents occur, rather than through anticipatory design strategies.

Additionally, the principle of accountability is treated more rigorously under the GDPR. Article 5(2) of the GDPR explicitly states that data controllers are responsible for, and must be able to demonstrate, compliance with all data protection principles. This includes documentation, policies, training, audits, and regular assessments. In contrast, the UU PDP mentions accountability in a more general sense, without requiring organizations to establish comprehensive governance structures or record-keeping systems that can demonstrate compliance on demand. This difference reflects the GDPR's maturity and its orientation toward enforceability and regulatory transparency, in contrast to the more formative stage of Indonesia's legal regime.

The transparency principle is extensively regulated in the GDPR. Detailed provisions on privacy notices, access rights, and mechanisms for ensuring informed consent are present throughout GDPR Articles 12–14. In contrast, Indonesia's PDP Law includes only general provisions on the obligation to inform data subjects, with less specific detail on format, language, timing, and content of such notices. This can pose challenges to ensuring meaningful consent and understanding among data subjects, especially in a country with vast linguistic, technological, and educational diversity.

The concept of special categories of personal data, or sensitive data, receives stronger emphasis under the GDPR (Art. 9). These categories such as health data, racial or ethnic origin, political opinions, religious beliefs, and biometric data require higher levels of protection and are subject to stricter processing conditions. While the

Indonesian PDP Law acknowledges similar types of sensitive data under Article 3(11), the regulatory treatment and protection mechanisms remain less robust. For instance, there is no dedicated requirement for conducting Data Protection Impact Assessments (DPIAs) before processing high-risk data, a procedure that is mandatory under GDPR Article 35 for certain types of sensitive data processing.

2. Data Subject Rights

One of the most defining and progressive features of the General Data Protection Regulation (GDPR) is its comprehensive protection of data subject rights, which is central to empowering individuals in the digital age. These rights, articulated in Articles 12 to 23 of the GDPR, reflect the foundational belief that individuals must maintain control over their personal data even after it is collected by data controllers. The rights include the right to access, rectify, erase (right to be forgotten), restrict processing, data portability, and the right to object. These provisions are designed not only to protect privacy but also to enhance transparency, autonomy, and accountability in data processing activities.

The Indonesian Personal Data Protection Law (UU PDP No. 27/2022) also incorporates a set of data subject rights in Articles 6 to 14, such as the right to be informed, the right to access, the right to correct data, the right to delete data, the right to limit processing, the right to withdraw consent, and the right to object to automated decision-making. This recognition represents a notable step forward in affirming individual digital rights within Indonesia's legal framework. However, while there is formal alignment in the types of rights recognized, significant differences exist in the scope, clarity, procedural detail, and enforceability of these rights when compared with the GDPR.

For instance, under Article 15 of the GDPR, the right of access is broadly defined to include not only the right to confirmation of whether data concerning the individual is being processed, but also detailed information such as the purposes of processing, the categories of personal data concerned, the recipients or categories of recipients, retention periods, the existence of data subject rights, and safeguards for international transfers. The Indonesian PDP Law, while acknowledging a right to access, does not provide the same granularity or specific procedural steps for individuals to exercise this right effectively. There are no explicit timeframes or standardized formats stipulated for how or when the data controller must respond, potentially leading to delays or refusals in practice.

The right to rectification is similarly recognized in both regimes. In the GDPR (Art. 16), individuals are granted the right to obtain the correction of inaccurate personal data and to have incomplete data completed. In Indonesia, the right is acknowledged in Article 10 of the PDP Law, but again, the lack of operational procedures, guidance, or enforcement protocols may limit its practical effectiveness. Without clear obligations on data controllers to promptly comply, individuals may find it difficult to ensure the accuracy of their personal data—an issue that can have significant consequences in contexts such as financial services, healthcare, or law enforcement.

A critical difference appears in the "right to erasure", or the so-called right to be forgotten, articulated in Article 17 of the GDPR. This right allows individuals to request the deletion of personal data where the data is no longer necessary for the original purpose, where consent is withdrawn, or where processing is unlawful. However, the

GDPR also provides important exceptions such as when data is needed to comply with a legal obligation, for reasons of public interest, or for the exercise of freedom of expression. These nuanced exceptions reflect the GDPR's attempt to balance privacy with other societal values. The Indonesian PDP Law similarly grants the right to erasure under Article 12, but fails to elaborate on such exceptions or establish balancing tests. This omission may lead to either over-deletion or unjustified refusal, depending on how data controllers interpret their obligations.

One of the most innovative rights under the GDPR is the right to data portability (Art. 20), which allows individuals to receive their personal data in a structured, commonly used, and machine-readable format, and to transmit it to another data controller. This right not only reinforces user control but also encourages competition and innovation, particularly in digital services and platform-based economies. In contrast, Indonesia's PDP Law does not explicitly recognize or detail this right, representing a significant gap in user empowerment and technological interoperability. Without mechanisms to support portability, individuals may face vendor lock-in or lack the freedom to switch service providers, especially in areas like telecommunications, digital banking, or social networking platforms.

Moreover, the right to object to processing, particularly for purposes such as direct marketing, profiling, or processing based on legitimate interests, is robustly protected under GDPR Article 21. Individuals may object at any time, and data controllers must immediately stop processing unless they can demonstrate compelling legitimate grounds. While Indonesia's PDP Law (Art. 14) provides for the right to object to automated decision-making, it lacks broader protections against general processing activities, including profiling for commercial or surveillance purposes. As algorithmic decision-making becomes more widespread, the absence of these protections raises concerns over transparency, fairness, and the potential for discriminatory outcomes.

3. Roles and Obligations of Data Controllers and Processors

A central pillar of both the General Data Protection Regulation (GDPR) and Indonesia's Personal Data Protection Law (UU PDP No. 27/2022) is the clear allocation of roles and responsibilities between entities involved in the processing of personal data. The GDPR makes a strong and clear distinction between a data controller and a data processor, who processes data on behalf of the controller (GDPR, Art. 4). This distinction is vital in attributing legal responsibility and in ensuring that data processing chains remain accountable at all levels. Controllers bear the primary duty to ensure that data processing activities comply with all relevant principles and legal obligations, while processors are also held to a high standard in terms of security, record-keeping, and cooperation with supervisory authorities.

Indonesia's PDP Law acknowledges similar distinctions in terminology, defining both "Pengendali Data Pribadi" (Data Controller) and "Prosesor Data Pribadi" (Data Processor) in Article 1. However, the level of regulatory clarity regarding their respective duties and liabilities is significantly less detailed than in the GDPR. While the law sets out general obligations for data controllers to protect personal data and ensure its lawful use, the specific procedural and operational obligations for both controllers and processors are not comprehensively articulated. This lack of specificity can lead to ambiguities in practice, particularly when multiple actors are involved in cross-border or cloud-based processing scenarios where the division of responsibility must be clearly demarcated.

One of the standout obligations under the GDPR is the requirement for data controllers and processors to maintain records of processing activities (Art. 30). These records serve as documentation of compliance and must include information such as processing purposes, data categories, recipients, international transfers, and security measures in place. Additionally, the GDPR mandates Data Protection Impact Assessments (DPIAs) for high-risk processing operations (Art. 35), such as those involving systematic monitoring, large-scale processing of sensitive data, or new technologies. DPIAs function as proactive risk assessment tools, helping organizations identify, evaluate, and mitigate privacy risks before data processing begins. In this regard, the GDPR promotes a preventive and risk-based approach to data governance.

Indonesia's PDP Law, although acknowledging the importance of data protection impact assessments, does not provide clear guidance on when and how DPIAs should be conducted. The term "impact assessment" is not explicitly defined or mandated in specific cases, leaving data controllers without regulatory direction on compliance thresholds or documentation standards. This omission weakens the law's preventive orientation and could result in organizations failing to adequately evaluate the privacy implications of their data processing activities, particularly in sectors such as fintech, health tech, or e-government where risks to data subjects can be substantial. Furthermore, the absence of mandatory DPIAs may hinder regulators from identifying systemic issues or preempting data breaches through oversight.

Another important area where the GDPR imposes significant duties is the appointment of a Data Protection Officer (DPO) (Arts. 37–39). Organizations engaging in large-scale processing of sensitive data, public authorities, and institutions whose core activities require regular and systematic monitoring are required to designate a DPO. This officer must possess expert knowledge of data protection law and practices, operate independently, and report to the highest management level. The DPO is a key actor in ensuring internal compliance, advising on obligations, and serving as a point of contact for regulators and data subjects. By contrast, the Indonesian PDP Law merely encourages the appointment of a DPO (Article 53), without making it mandatory or establishing criteria for their qualifications, independence, or institutional role. As a result, many organizations in Indonesia may overlook the strategic value of appointing a DPO, potentially weakening internal accountability and diminishing the quality of responses to data protection challenges.

4. Supervisory Authority and Enforcement

The GDPR provides a robust enforcement framework, supported by independent supervisory authorities in each EU member state. These authorities have investigative, corrective, and advisory powers, and are coordinated by the European Data Protection Board (EDPB) to ensure consistency (GDPR Arts. 51–67). Furthermore, the GDPR allows for significant administrative fines, with penalties reaching up to €20 million or 4% of global annual turnover, whichever is higher (Art. 83).

In contrast, Indonesia's data protection supervisory body under the PDP Law is still in developmental stages. According to Article 58 of the law, a supervisory authority is to be established by the President, but its operational framework, independence, and technical capacity remain unclear as of 2024. Without an established and empowered supervisory body, law enforcement and compliance assurance remain

weak. Furthermore, while Indonesia's PDP Law includes administrative and criminal sanctions, the maximum fines (e.g., up to 2% of annual revenue) and enforcement mechanisms are not yet fully operational or integrated into institutional practices.

5. Cross-Border Data Transfers

Cross-border data transfer is a crucial issue in data protection law, especially in the context of cloud services, global social media platforms, and international e-commerce. The GDPR has strict rules requiring an adequate level of protection in the recipient country, based on adequacy decisions by the European Commission or through mechanisms such as Standard Contractual Clauses and Binding Corporate Rules (GDPR Chapter V). Indonesia's PDP Law, in Article 55, also regulates cross-border data transfer. However, its provisions are less comprehensive. It stipulates that the recipient country must have an adequate data protection level, but there is no detailed process or criteria for determining adequacy, nor are there defined alternative safeguards as in the GDPR. This could potentially limit Indonesia's ability to participate fully in global data ecosystems or complicate legal certainty for multinational companies operating in Indonesia.

6. Legal Culture, Enforcement Practice, and Institutional Readiness

Beyond textual analysis, practical enforcement and institutional readiness are key differentiators between the GDPR and Indonesia's PDP Law. The European Union has invested heavily in building a strong data protection culture, with a track record of high-profile enforcement actions and public awareness campaigns. For example, the Irish Data Protection Commission fined Meta over €1.2 billion for GDPR violations in 2023, indicating serious regulatory commitment (EDPB, 2023). Indonesia, on the other hand, still faces challenges related to public awareness, regulatory capacity, and institutional integrity. Many individuals are unaware of their data rights, and businesses often treat data protection as a compliance burden rather than an ethical obligation. Moreover, the lack of established case law and administrative precedent limits the predictability and maturity of enforcement.

CONCLUSION

This study has demonstrated that while both the General Data Protection Regulation (GDPR) and Indonesia's Personal Data Protection Law (UU PDP No. 27/2022) share foundational principles in protecting personal data, significant differences remain in terms of regulatory depth, enforceability, and institutional maturity. The GDPR provides a more comprehensive, structured, and enforceable legal framework, supported by detailed procedural safeguards, strong supervisory authorities, and a culture of compliance. In contrast, Indonesia's PDP Law, though an important milestone in national data governance, still lacks clarity in key areas such as data subject rights implementation, roles and obligations of data controllers and processors, cross-border data transfers, and independent oversight. For Indonesia to fully realize the protective potential of its law and align with international best practices, future efforts must focus on developing clear implementing regulations, establishing a robust and independent data protection authority, enhancing public and corporate awareness, and building the technical and institutional capacity necessary for effective enforcement. Only then can Indonesia ensure that individuals' digital rights are respected and protected in the face of rapid technological change and global data flows.

Reference

Almunawar, M. N., & Anshari, M. (2022). Data privacy and personal data protection in Indonesia: A legal and regulatory overview. Journal of Law and Data Protection, 5(2), 134–148.

Bennett, C. J. (2018). The governance of privacy: Policy instruments in global perspective (2nd ed.). MIT Press.

Custers, B., Dechesne, F., Sears, A. M., Tani, T., & van der Hof, S. (2019). A comparison of data protection legislation and policies across the EU. Computer Law & Security Review, 35(4), 105314. https://doi.org/10.1016/j.clsr.2019.05.003

European Parliament & Council of the European Union. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). Official Journal of the European Union, L119, 1–88.

Greenleaf, G. (2021). Global data privacy laws 2021: Despite COVID delays, 145 laws show GDPR dominance. Privacy Laws & Business International Report, 170, 10–13.

Indonesian Government. (2022). Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi. Lembaran Negara Republik Indonesia Tahun 2022 Nomor 200.

Kamarinou, D., Millard, C., & Singh, J. (2016). Machine learning with personal data: Is data protection law smart enough to meet the challenge? International Data Privacy Law, 6(2), 77–97. https://doi.org/10.1093/idpl/ipw003

Lynskey, O. (2015). The foundations of EU data protection law. Oxford University Press.

Marelli, L., & Testa, G. (2020). Scrutinizing the EU General Data Protection Regulation: New rights, old challenges in data protection. Bioethics, 34(7), 620–628. https://doi.org/10.1111/bioe.12798

Mitchell, R. (2020). GDPR enforcement in practice: Fines, consistency, and data subject rights. Information & Communications Technology Law, 29(3), 293–309. https://doi.org/10.1080/13600834.2020.1788979

Nasution, A. Z., & Pratama, Y. (2023). Comparative analysis of personal data protection regulation: Indonesia and the European Union. Indonesian Journal of Law and Technology, 4(1), 51–68.

Purnama, D. (2023). Tantangan implementasi UU Perlindungan Data Pribadi: Analisis kesiapan lembaga dan penegakan hukum. Jurnal Hukum dan Teknologi, 6(2), 233–248.

Rachman, T. (2022). Data sovereignty and cross-border data transfer in the era of globalization: Indonesia's legal framework. Jurnal Konstitusi, 19(4), 665–684.

Svantesson, D. J. B. (2020). Solving the Internet jurisdiction puzzle. Oxford University Press.

Wright, D., & Raab, C. (2014). Privacy principles, risks and harms. International Review of Law, Computers & Technology, 28(3), 277–298. https://doi.org/10.1080/13600869.2014.919529