ABDURRAUF JOURNAL OF ISLAMIC STUDIES
https://journal.staisar.ac.id/index.php/arjis
Vol. 5, No. 3, 2026, pp. 274-292
P-ISSN (Print) 2828-3597 | E-ISSN (Online) 2828-4879
DOI: 10.58824/arjis.v5i3.648

Symbolic Law, Substantial Gaps: Reassessing Indonesia's Personal Data Protection Law in Light of the GDPR (General Data Protection Regulation) Effectiveness and Adequacy Standards

Rizkita Kurnia Sari[1*], Happy Yulia Anggraeni[2], Erna Listiawati[2]
[1-2] Universitas Islam Nusantara, Indonesia
[3] Universitas Padjajaran, Indonesia
*Corresponding Author: rizkitasari311@gmail.com

Article Info
Received: 03-09-2026
Revised: 11-10-2026
Accepted: 13-10-2026
Published: 14-10-2026

Keywords:
Adequacy; GDPR; Legal Effectiveness; PDP Law; Personal Data Protection

Abstract
The rapid development of information technology has driven the commodification of digital data and increased global privacy vulnerabilities. The European Union has responded through the General Data Protection Regulation (GDPR), which uses the doctrine of adequacy decisions to assess the equivalence of personal data protection across countries, while Indonesia has enacted Law No. 27 of 2022 on Personal Data Protection (PDP Law). Using a normative and comparative legal approach, this study evaluates the alignment of norms as well as the effectiveness of the legal protections provided by the PDP Law and its implementing regulation (Government Regulation No. 33 of 2026) against GDPR standards in the areas of data subject rights, data controller obligations, independent oversight, enforcement, and cross-border data transfers. The analysis reveals that the PDP Act has adopted the fundamental principles of the GDPR; however, significant gaps remain regarding the independence of the supervisory authority, the rationalization of fines, and the governance of cross-border data transfers. These gaps are exacerbated by limited institutional capacity and low compliance awareness, resulting in data subject rights that tend to be declaratory rather than enforceable. This study concludes that the PDP Law does not yet fully meet the European Union′ s adequacy criteria. The study′ s contributions are both theoretical, in the form of an integrated analytical framework combining normative equivalence and enforcement effectiveness and practical in the form of recommendations for the establishment of an independent supervisory authority, adequacy assessment procedures, and the strengthening of sanctions enforcement for Indonesian policymakers.

Info Artikel

Kata Kunci:
Adekuasi; GDPR; Efektivitas Hukum; UU Pelindungan Data Pribadi (UU PDP); Pelindungan Data Pribadi

Abstrak
Pesatnya perkembangan teknologi informasi telah mendorong komodifikasi data digital dan meningkatkan kerentanan privasi global. Uni Eropa menjawabnya melalui General Data Protection Regulation (GDPR) yang menggunakan doktrin *adequacy decisions* untuk menilai kesetaraan perlindungan data pribadi antarnegara, sedangkan Indonesia mengesahkan Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP). Dengan pendekatan yuridis normatif dan komparatif, penelitian ini mengevaluasi

keselarasan norma sekaligus efektivitas pelindungan hukum UU PDP beserta peraturan pelaksanaannya (PP Nomor 33 Tahun 2026) terhadap standar GDPR pada aspek hak subjek data, kewajiban pengendali data, pengawasan independen, penegakan hukum, dan transfer data lintas negara. Hasil analisis menunjukkan bahwa UU PDP telah mengadopsi prinsip fundamental GDPR, tetapi masih terdapat kesenjangan signifikan pada independensi otoritas pengawas, rasionalisasi sanksi denda, dan tata kelola transfer lintas negara. Kesenjangan tersebut diperberat oleh keterbatasan kapasitas kelembagaan dan rendahnya kesadaran kepatuhan, sehingga hak subjek data cenderung bersifat deklaratif ketimbang dapat ditegakkan. Penelitian ini menyimpulkan bahwa UU PDP belum sepenuhnya memenuhi kriteria adequacy Uni Eropa. Kontribusi penelitian ini bersifat teoretis, berupa kerangka analisis terpadu yang menggabungkan kesetaraan normatif dan efektivitas penegakan, serta praktis, berupa rekomendasi pembentukan otoritas pengawas independen, prosedur penilaian *adequacy*, dan penguatan penegakan sanksi bagi pembentuk kebijakan Indonesia.

Copyright© 2026 by Author(s)
This work is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License.

INTRODUCTION

Advances in information and communication technology during the digital age have brought about a major transformation in the way personal information is collected, stored, and processed. Virtually all activities in contemporary society rely on the exchange of personal information through various digital platforms, including e-commerce services, social media, and online financial transactions. This situation exposes personal information to potential misuse, including data breaches, identity theft, and the processing of personal data without proper authorization (Wibowo et al., 2024). Personal information has become a valuable resource that is frequently used in online transactions, government services, and commercial operations. Nevertheless, its prevalence continues to rise. The use of personal information also poses potential risks, including misuse, unauthorized disclosure, and illegal data trading (Elza, 2025).

Data breaches are on the rise globally, as highlighted in a Statista report, which shows an increase of nearly 15% in such incidents from 2019 to 2022. The sectors most affected by data breaches are primarily healthcare, finance, and technology, as these fields handle large amounts of sensitive information. In Southeast Asia, Indonesia is one of the countries most vulnerable to data breaches. This is evidenced by the fact that Indonesia has more than 200 million online users, with internet penetration reaching 77% in 2023 (Kriswandaru et al., 2024).

Several countries have adopted stronger laws regarding the protection of personal information to address growing risks. One of the first organizations to adopt such legislation was the European Union, which introduced the General Data Protection Regulation (GDPR) in 2018. The GDPR has been described as the global standard for personal data protection because it provides a framework for governing data processing principles, data subject rights, data controller responsibilities, and robust enforcement measures (Absor, 2023).

From a legal perspective, personal data protection consists of two main components: The first component is the protection of personal data as an asset vulnerable to misuse, and the second component refers to the right to privacy as a fundamental right of every individual. This is stipulated in Article 28G, paragraph (1) of the 1945 Constitution of Indonesia as follows:

1. Protection of Personal Data as a Protected Interest

Personal data is regarded as part of a person's property or property interests, which has economic and social significance, and therefore requires protection from all forms of misuse, theft, unlawful use, or other violations

2. Protection of the Right to Privacy as a Human Right
   Personal data is directly linked to the right to privacy. This gives individuals the right to control the collection, processing, transfer, and storage of their personal data. The government has an obligation to provide protection against any violation of the right to privacy.

All of these requirements are reinforced by Law No. 27 of 2022 on Personal Data Protection, which governs the rights of data subjects, the responsibilities of data controllers, the processing of personal data, and penalties for personal data violations. The legal framework underlying Law No. 27 of 2022 is democratic and adaptive, and aligns with the values enshrined in the philosophy of the Indonesian nation (Fauzy & Shandy, 2022).

From the government's perspective, Indonesia has enacted Law No. 27 of 2022 on Personal Data Protection (PDP Law), which indicates that Indonesia has taken steps to provide legal protection for personal data. The enactment of the PDP Law demonstrates that Indonesia is ready to face the challenges of the digital age.

Personal data refers to any data that can lead to the direct or indirect identification of an individual. Some examples of personal data include names, addresses, national ID card (KTP) numbers, phone numbers, health records, and online preferences. In today's world, where technology is at its peak, this data is not only used for administrative purposes but is also targeted for manipulation and misuse by organizations and criminals through cybercrime. Incidents such as the data breach involving 279 million people from BPJS Kesehatan, the data breach at Tokopedia, and the sale of data on illegal forums demonstrate the need for strict regulations and their enforcement (Nusantara et al., 2024).

From the government's perspective, Indonesia has enacted Law No. 27 of 2022 on Personal Data Protection (PDP Law), which indicates that Indonesia has taken steps to provide legal protection for personal data. The enactment of the PDP Law demonstrates that Indonesia is ready to face the challenges of the digital age. Indonesian society today relies heavily on information technology-based media to store personal data or transmit it to others. This influences how data is misused, leading to violations of personal data protection. The Personal Data Protection Law is intended to meet the public's need for security and ensure the protection of the personal data of the Indonesian people, while also putting an end to the misuse of personal data (Manurung & Thalib, 2022).

However, even though this law has evolved into a national legal instrument, it remains unclear to what extent it is compatible with international norms and standards, particularly those related to the GDPR framework. One key term in this context is "adequacy," defined as an assessment of whether data protection measures in another country's legal system are sufficient compared to EU data protection standards under Article 45 of the GDPR. The importance of this term lies in its role in facilitating cross-border data transfers. Under Article 45 of the GDPR, transfers to a third country are permitted when the European Commission issues an "adequacy decision," meaning that the country in question has data protection standards equivalent to those of the EU (Rahman & Mulyani, 2025).

Kuner explained that the GDPR's data transfer framework aims to ensure that personal data transferred to a third country remains protected at a level equivalent to EU standards (Kuner, 2013). In addition to the aspect of adequacy, the effectiveness of legal protection is also a key concern in this regard. It is important to remember that effectiveness is determined not only by the

existence of laws, but also by the implementation and enforcement of the law, supervisory bodies, and the level of compliance among data processors. According to (Soekanto (2008) in Fachran et al., 2026), the effectiveness of the law is influenced by several factors, such as the substance of the law, law enforcement, infrastructure, society, and legal culture. Therefore, a comprehensive analysis must be conducted to determine whether the protections provided by Indonesia's Personal Data Protection Act (UU PDP) are effective and in line with the GDPR (Soekanto (2008) in Fachran et al., 2026).

Existing scholarship has largely examined the PDP Law either as a descriptive account of data subject rights and controller obligations (Manurung and Thalib 2022; Fauzy and Shandy 2022) or in terms of the general theory of GDPR transfer mechanisms (Kuner 2013), and recent work has begun to link the absence of an independent supervisory authority to weak enforcement (Fachran et al. 2026). Yet the state of the art has moved quickly: Government Regulation No. 33 of 2026, promulgated on 16 July 2026, now assigns adequacy assessments to a future data protection authority that will keep a " whitelist" of adequate jurisdictions (Rajah & Tann Asia 2026), while the authority itself and the list do not yet exist (HLC 2026). The research gap is that no study has tested the PDP Law and this implementing regulation against the adequacy criteria of Article 45 GDPR, as elaborated in the EDPB' s adequacy referential (European Data Protection Board 2018), together with an effectiveness lens drawn from Soekanto' s five factors (Soekanto 2008). The novelty of this study lies in combining these two analytical frames, normative equivalence and effectiveness in practice, to examine the PDP Law as completed by its newest implementing rules, rather than the statute alone. Accordingly, this study aims to determine whether the PDP Law meets the adequacy standard, to compare the effectiveness of data subject rights, controller obligations, and enforcement mechanisms with their GDPR counterparts, and to identify the legal implications of the remaining gaps for cross-border data transfers. Its contribution is twofold: theoretically, an integrated adequacy-effectiveness framework for assessing data protection regimes in developing jurisdictions; and practically, evidence-based recommendations for the design of Indonesia' s supervisory authority and adequacy procedures.

Based on this discussion, it can be concluded that this study is important for assessing the compatibility of Indonesia's Personal Data Protection Law with the GDPR in terms of the adequacy and effectiveness of legal protection, in order to provide an overview of Indonesia's status regarding personal data protection on the international stage and to offer recommendations for future policies.

1. Do the personal data protection provisions in the PDP Act meet the "adequacy" standard as set forth in the GDPR?
2. How do the provisions regarding data subject rights, data controller obligations, and enforcement mechanisms in the PDP Act compare to those in the GDPR in terms of effectiveness?
3. What are the legal implications of the regulatory gaps between the PDP Act and the GDPR for personal data protection in the context of cross-border data transfers?

This study will be conducted to determine whether the Personal Data Protection Act (UUPDP) meets the "adequacy" requirement, which forms the basis of the General Data Protection Regulation (GDPR). In addition, the researcher will compare the effectiveness of provisions regarding data subjects' rights and data controllers' obligations under the Personal Data Protection Act and the GDPR, as well as identify the legal implications of regulatory differences between the two regarding personal data protection in the context of cross-border data transfers. The GDPR stipulates that, pursuant to Article 45 of the GDPR, for a country to receive an

adequacy decision, it must ensure adequate protection of personal data, which means having comprehensive data protection regulations, data subject rights, an independent supervisory authority, effective enforcement mechanisms, regulations on cross-border transfers of personal data, and adequate sanctions.

RESEARCH METHOD

This study employs the normative legal research (doctrinal legal research) through a literature review of positive legal norms (Satory et al. 2024). It combines the statutory approach and the comparative approach to analyze Law No. 27 of 2022 on Personal Data Protection (PDP Law), together with its implementing regulation, Government Regulation No. 33 of 2026, against the General Data Protection Regulation (GDPR). The primary legal materials are these instruments, and the secondary materials are scholarly literature and the European Data Protection Board′ s adequacy referential. Adequacy is assessed against the criteria of Article 45 GDPR, as elaborated by the European Data Protection Board (2018): (1) core data protection principles and definitions; (2) data subject rights; (3) controller and processor obligations, including accountability and rules on onward transfers; (4) an independent supervisory authority; and (5) enforcement mechanisms, including redress and sanctions. Effectiveness is assessed through Soekanto′ s (2008) five factors: the substance of the law, law enforcement, supporting facilities and infrastructure, society, and legal culture. These indicators are applied to each provision compared, and the results are analyzed qualitatively to identify regulatory gaps and their implications for cross-border data transfers.

Data sources consist of primary legal materials, namely Law No. 27 of 2022 on Personal Data Protection (PDP Law) and Regulation (EU) 2016/679 (GDPR), supplemented by Government Regulation No. 33 of 2026 as its implementing instrument, as well as secondary legal materials such as reputable legal journals, textbooks, and relevant policy papers. All legal materials were analyzed qualitatively using a descriptive-analytical method (Creswell and Creswell,, 2023) with deductive reasoning, operationalized through systematic-grammatical interpretation and a legal gap analysis of crucial clauses to assess the adequacy of protection (Simanjuntak 2024). Within the doctrinal tradition (Satory et al., 2024), the two regimes are compared functionally, that is, by the legal problems they address rather than by textual similarity alone (Siems, 2022). Through this comparative synthesis, the study produces prescriptive conclusions in the form of solution-oriented recommendations for institutional restructuring and the improvement of the regulatory governance of personal data protection in Indonesia.

RESULTS AND DISCUSSION

Compliance with the Adequacy Standard in Law No. 27 of 2022 on Personal Data Protection Based on the General Data Protection Regulation (GDPR)

With advances in information and communication technology, there has been an increase in cross-border processing of personal data. Therefore, regulations are needed to ensure adequate protection of personal data. At the international level, one of the main benchmarks is the General Data Protection Regulation (GDPR) (Chong, 2026). The GDPR establishes criteria for determining adequacy in situations where the level of personal data protection in a given country is equivalent to that of the EU. Indonesia has enacted Law No. 27 of 2022 on Personal Data Protection as the national regulation governing personal data protection in Indonesia. Marelli (2024) explain that the adequacy mechanism under European Union law is used to evaluate whether personal data protection in a third country meets EU data protection standards, thereby enabling secure and lawful cross-border data transfers.

DOI: 10.58824/arjis.v5i3.648

The rules regarding the adequacy criteria under the GDPR can be found in Article 45 of the GDPR. According to Article 45, personal data may only be transferred if there is an adequate level of protection in the third country. The factors used by the European Commission in determining adequacy include:

a. The principles of the rule of law and human rights;
b. The Personal Data Protection Act;
c. The efficiency of independent supervisory bodies;
d. Law enforcement and dispute resolution processes; and
e. Provisions to ensure the security of cross-border data transfers.

Recent scholarship emphasizes that the adequacy mechanism under the GDPR requires a third country's legal framework to provide a level of personal data protection that is essentially equivalent to that guaranteed within the European Union. This assessment extends beyond the existence of legislation and includes institutional oversight, enforcement mechanisms, and effective remedies for data subjects. Consequently, the adequacy framework is designed to ensure that cross-border transfers of personal data do not diminish the level of protection guaranteed by the GDPR, thereby enabling lawful international data flows while safeguarding fundamental privacy rights (Rahman & Mulyani, 2025).

The adequacy provision is most evident in Indonesia's Personal Data Protection Act when it regulates cross-border transfers of personal data. According to Article 56 of the Personal Data Protection Act, a personal data controller may transfer personal data to a controller or processor outside Indonesia as long as the foreign jurisdiction maintains data protection standards that are equal to or higher than those set forth in the Personal Data Protection Act.

This provision demonstrates that Indonesia applies the principle of adequacy in a manner similar to the GDPR. If the destination country does not provide an equivalent level of protection, the data controller must ensure that adequate and binding safeguards are in place. Failure to meet these two requirements means that data transfers may only take place after obtaining the data subject's consent. This rule applies a three-tiered protection approach as follows: protection based on the recipient country, the existence of binding safeguards, or the data subject's consent. The concept is similar to international data transfers under the GDPR.

Similarities Between the PDP Act and the GDPR in Ensuring Compliance with Adequacy Requirements:

a. Recognition of Data Subjects'

   Rights Under the PDP Law, certain rights have been granted to data subjects, such as the right to access information, the right to correct information, the right to erasure, and the right to withdraw consent. These rights are similar to those granted under the GDPR, as the GDPR also recognizes data subjects' rights. Articles 5 through 16 of the PDP Act regulate the rights of data subjects as a means of protecting individual privacy.

b. Principles of Data Processing

   According to Article 16 of the Data Processing Act, data processing must be carried out in a limited, specific, lawful, transparent, accurate, and responsible manner. These principles are the same as those of the GDPR, namely lawfulness, fairness, transparency, and data minimization.

c. Obligations of Data Controllers

   The Data Processing Act sets forth the obligations of data controllers to safeguard individuals' privacy and personal data. In accordance with Article 39 of the Data Processing Act, reliable and responsible security systems must be used to protect

individuals' personal data. The aforementioned regulations align with the GDPR's principles of integrity and confidentiality.

d. Regulations on Cross-Border Transfer of Personal Data

In accordance with Article 56 of the Data Processing Law, adequacy-based cross-border transfers of personal data are regulated, similar to the provisions set forth in Article 45 of the GDPR. Although the Data Protection Law (PDP) has incorporated the concept of adequacy, there are several differences compared to the GDPR.

e. Lack of an Independent Supervisory Authority

Under the GDPR, there must be an independent supervisory authority. In Indonesia, however, data protection oversight authority is still in the development stage. This situation will pose challenges in obtaining international recognition of adequacy.

f. Incomplete Implementing Regulations

For the implementation of the PDP Act, implementing regulations are still needed to facilitate the process. Without these regulations, data protection requirements could give rise to legal issues.

g. Law Enforcement

It is known that the GDPR enforces a very strict system of administrative sanctions. Although administrative and criminal sanctions are stipulated in the PDP Act, the issue lies in the readiness of the relevant agencies to enforce the law.

Normatively, there are indications that the PDP complies with the requirements set by the GDPR, including: protection of data subjects' rights, data processing principles, data controller obligations, and adequate cross-border data transfers. However, this compliance does not automatically guarantee adequacy as recognized by the international community. With regard to the GDPR, adequacy is based not only on the existence of legislative provisions but also on their actual implementation and the supervisory body. This indicates that Indonesia must take further steps, such as establishing an independent supervisory body, developing implementing regulations, enhancing digital law enforcement, and strengthening international cooperation.

To assess whether Indonesia′ s framework meets the adequacy standard, the PDP Law is compared with the GDPR across the five aspects that Article 45 GDPR and the EDPB′ s adequacy referential treat as central: data subject rights, processing principles, independent supervision, law enforcement, and cross-border transfers. Table 1 summarizes these provisions and, for each aspect, assesses not only the equivalence of the norms but also their effectiveness in practice, since adequacy depends on how the law is supervised and enforced.

Table 1. Comparison of the PDP Law and the GDPR Based on the Adequacy Criteria

Aspect	PDP Law (Law No. 27 of 2022)	GDPR (Regulation (EU) 2016/679)	Brief Analysis
Data subject rights	Arts. 5–15: right to information, access, rectification, erasure, withdrawal of consent, objection to automated decision-making, restriction, compensation, and data portability.	Arts. 12–23: transparency, access, rectification, erasure, restriction, portability, objection, and rights regarding automated decision-making; remedies in Arts. 77–82.	Normatively close, so this aspect is the PDP Law's strongest. The difference is in effectiveness: under the GDPR, rights are backed by a supervisory authority and a clear complaint route, while the PDP Law lacks a functioning body to receive and resolve complaints.
Processing principles	Art. 16: limited and specific, lawful, transparent, accurate, accountable, secure, and purpose-bound processing. Lawful bases are in Art. 20.	Art. 5: lawfulness, fairness, transparency, purpose limitation, data minimisation, accuracy, storage limitation, integrity and confidentiality,	Substantively equivalent. The PDP Law is less explicit on storage limitation and does not codify "fairness" as a separate principle. Equivalence on paper is not yet equivalence in practice.

		accountability. Lawful bases are in Art. 6.	
Independent supervision	Arts. 58–60 provide for a data protection agency that reports to the President. A draft presidential regulation was released in February 2026, and as of mid-2026 the agency was still not in place (Rajah & Tann Asia 2026).	Arts. 51–59: independent supervisory authorities with investigative, corrective, and sanctioning powers; independence is guaranteed in Art. 52.	This is the main obstacle to adequacy. Independence is an explicit criterion in Art. 45(2)(b), and an agency that reports to the executive raises doubts about its autonomy.
Law enforcement	Art. 57 (administrative sanctions, including fines of up to 2% of annual revenue) and Arts. 67–73 (criminal sanctions). Enforcement currently relies on general courts.	Art. 83: fines of up to EUR 20 million or 4% of worldwide annual turnover; corrective powers in Art. 58; judicial remedies in Arts. 78–79.	Sanction ranges are comparable, but the PDP Law has no body to impose them consistently. A strong sanction norm without an enforcer weakens its deterrent effect.
Cross-border transfers	Art. 56: equivalent or higher protection in the destination country, then binding safeguards, then data subject consent. GR 33/2026 (Arts. 160–174) gives the DPA the adequacy assessment and a "whitelist" (Rajah & Tann Asia 2026).	Chapter V: adequacy decision by the European Commission (Art. 45), appropriate safeguards (Art. 46), derogations (Art. 49).	The structure is similar (three tiers), but there is a procedural gap. The adequacy list and standard contractual clauses depend on a DPA that does not yet exist (HLC 2026).

Source: Compiled by the Author (2026)

A Comparison of the Effectiveness of Provisions Regarding Data Subjects' Rights, Data Controllers' Responsibilities, and Enforcement Provisions Under the Personal Data Protection Act (PDP) and the GDPR

The advent of digital technology and cross-border information exchange has heightened the need to protect personal data. Personal data has become a critical asset that holds monetary value and is also linked to individuals' right to privacy (Aura et al., 2025). Consequently, countries around the world have begun enacting laws to regulate the management of personal data. The European Union's General Data Protection Regulation (GDPR) has been recognized as the international benchmark for personal data protection, as it outlines the rights of data subjects, the obligations of data controllers, and strict enforcement procedures (Cejas et al., 2025). Law No. 27 of 2022 on Personal Data Protection (PDP Law) has been enacted in Indonesia. Although the PDP Law reflects a desire to align the national legal framework with international legal frameworks, particularly the GDPR, there are significant differences in its effectiveness, especially from institutional, technical, and enforcement perspectives.

The General Data Protection Regulation (GDPR), or Regulation (EU) 2016/679, is a European Union regulation governing the protection of personal data. Articles 12 through 23 of the GDPR specifically address the rights of data subjects. These provisions aim to give individuals greater control over their personal data. In terms of data subject rights, the GDPR provides very broad protection. The provisions regarding these rights are set forth in Articles 12 through 23 of the GDPR. These rights include:

1. the right to information;
2. the right of access;
3. the right to rectification;
4. the right to erasure (right to be forgotten);
5. the right to restrict processing;
6. the right to data portability;
7. the right to object to processing; and
8. rights related to automated decision-making

DOI: 10.58824/arjis.v5i3.648

Article 12 requires that the obligation to inform data subjects be fulfilled in such a way that the information is: clear, easy to understand, concise, and accessible. Data controllers are required to: respond to requests from data subjects without undue delay, respond no later than one month, and not charge any fees for responding unless the request is clearly unfounded or excessive. Article 12 emphasizes the principle of transparency in the handling of personal data.

Article 13 sets forth the information that must be provided when data is collected from data subjects. This information includes: the identity of the data controller; the purpose of data processing; the lawful basis for data processing; the recipients of the data; the data retention period; the rights of data subjects; and the data subjects' right to file a complaint. The purpose is to ensure that individuals are aware of how their personal data will be used.

If personal information is collected indirectly and not obtained from the data subject, such as from a third party, an organization, or public records then Article 14 applies. The controller must provide the following information regarding the data: the source of the data, the type of data, and the purpose of processing. This information must be provided within one month of the data's collection. Under Article 15, the rights of data subjects include: the right to be informed if personal data about them is being processed; the right to receive a copy of their personal data; the right to know the purpose of the data processing; and the right to know who will receive their personal data. In accordance with Article 15, data subjects have the right to obtain confirmation from the controller as to whether or not personal data concerning them is being processed. This right of access is intended to enhance individuals' control over their data.

Article 16 grants data subjects the right to correct their personal data if it is: inaccurate, incomplete, or outdated. The data controller must comply with such requests without delay. Article 17 outlines the right to erasure of personal data ("the right to be forgotten"). Data subjects may claim the right to erasure if: the data is no longer necessary; consent has been withdrawn; the processing is unlawful; or the data is used for direct marketing and the data subject objects to such use. This right does not apply when the data is still necessary for: legitimate interests; freedom of expression; public interest; or scientific research. This article is among the most popular ones based on the GDPR.

Under Article 18, data subjects have the right to request that data processing be restricted if: the accuracy of the data is disputed; the processing is unlawful; or the data is required for legal reasons. The restriction may only be applied for the intended purpose during that period. Under Article 19, the data controller is required to notify recipients regarding personal data if: corrections are made to the data; or the data is deleted; or the processing of the data is restricted. This is intended to ensure that all changes made to the data are applied universally.

Article 20 states that data subjects have the following rights: the right to obtain their personal data in electronic form; and the right to transfer the data to another controller. These two rights apply when data processing is carried out by automated means. Article 21 grants individuals the right to object to the processing of their personal information, particularly when it is used for: marketing purposes, legitimate interests, or profiling. An objection may only be upheld if the controller cannot provide a valid legal basis for the processing.

Article 22 protects individuals from any decisions made automatically without human involvement, including profiling. Data subjects have the right to: be free from automated processing, request human intervention, and object. Some examples include: automated credit denial, automated hiring, and risk assessment. This provision is particularly important in the era of artificial intelligence. Article 23 allows EU Member States to impose restrictions on the rights of data subjects in certain situations for the following purposes: national security, national defense,

public safety, crime prevention, and the protection of public interests. These restrictions are subject to the following conditions: they must be legally justified, proportionate, and respect human rights.

Articles 12 through 23 of the GDPR indicate that the main features of this regulation include:

1. Protection of privacy rights;
2. Transparency in data processing;
3. Control over personal data;
4. Accountability of the data controller.

Lee A. Bygrave states that the purpose of modern data protection laws is to enable individuals to exercise control over their personal information. Therefore, the GDPR not only regulates corporate responsibilities but also strengthens the position of individuals as owners of their personal data. Indonesia's Personal Data Protection Act regulates the rights of data subjects primarily through Sections 5–16. These include: the right to information, the right to access personal data, the right to correct errors, the right to withdraw consent, the right to erasure of personal data, the right to restrict processing, and the right to seek compensation.

Article 5(1) of the PDP Act stipulates that data subjects whose data is processed have the right to receive information regarding the clarity of their identity, the legitimate grounds for processing, and the purposes of processing their personal data. Similarly, Article 8 of the PDP Law establishes the right to stop the processing of and to have one's personal data erased. The recognition of these rights demonstrates that Indonesia applies internationally accepted data protection principles, influenced by the GDPR.

Textually, the discrepancy between Articles 5–16 of the PDP Law and Articles 12–23 of the GDPR appears minor: both regimes recognize the rights to information, access, rectification, erasure, and restriction of processing. However, this textual equivalence must be tested using the "law in the books versus law in action" approach (Pound, 1910), because a subjective right in administrative law is meaningful only to the extent that it is justiciable—that is, enforceable through clear and independent mechanisms. Under the GDPR, these rights are underpinned by three interlocking functional elements: (i) precise procedural obligations for the controller (a one-month deadline, a prohibition on fees, and the obligation to notify third parties under Article 19); (ii) independent supervisory authorities in each member state (Article 51) that can receive complaints and impose corrective sanctions; and (iii) the right to judicial remedy that data subjects can pursue directly. The PDP Law, by contrast, sets forth the same rights normatively (Articles 5, 8) but has not yet incorporated these three supporting elements on an equal footing, the Indonesian supervisory authority remains a functional-transitional body under the Ministry, rather than an independent body with investigative and corrective powers equivalent to those under Article 58 of the GDPR.

Thus, the real difference between the two regimes does not lie in the substance of the rights (Articles 5–16 of the PDP Act are normatively compatible with Articles 12–23 of the GDPR), but rather in the enforcement framework, meaning that data subjects' rights under the current PDP Act are more accurately categorized as declaratory rights rather than enforceable rights as defined within the GDPR framework.

The GDPR places many responsibilities on data controllers, particularly in Articles 24 through 43. Controllers must: implement appropriate safeguards for processing activities; maintain records of processing activities; conduct a Data Protection Impact Assessment (DPIA); appoint a Data Protection Officer (DPO), if necessary; and notify any personal data breaches within 72 hours. Article 24 of the GDPR states that controllers must take appropriate technical and

organizational measures to ensure that processing is carried out in accordance with this Regulation (European Union, 2016).

According to Christopher Kuner, auditors are not only required to follow the rules, but must also be able to demonstrate their compliance. Articles 20–53 of the PDP Act set forth the obligations of data controllers. They are required to: process data in a lawful and transparent manner; ensure confidentiality and security; prevent unauthorized access; report data breaches; and delete or destroy data after the retention period has expired. Article 35 of the PDP Act stipulates that personal data controllers are required to safeguard and secure the personal data they are processing. Furthermore, Article 46 mandates notification to data subjects in the event of a data protection breach.

The most significant difference between Article 35 of the PDP Law and Article 24 of the GDPR lies not in the presence or absence of security obligations, but in the nature of the standards applied. Article 24 of the GDPR adopts a risk-based approach that requires the controller to actively demonstrate compliance, through processing documentation, a DPIA, and the appointment of a DPO, so that the burden of proof for compliance rests with the controller (accountability as a demonstrable obligation, as emphasized by Kuner). Article 35 of the PDP Law, with the phrase "reliable and responsible security systems," formulates the same obligation in an outcome-based manner without measurable operational parameters. From a legal reasoning perspective, a norm that does not include technical standards and mechanisms of proof risks becoming a vague norm that is difficult to use as a basis for administrative enforcement or criminal liability, because supervisory authorities lack objective benchmarks to assess non-compliance. Consequently, even though the PDP Law textually "adopts" the GDPR's principle of accountability, doctrinally it has not yet achieved the same function, because accountability under the GDPR is self-executing (it can be directly verified through compliance documentation), whereas under the PDP Law it remains dependent on implementing regulations that have not yet been issued.

Comparison of Law Enforcement:

a. Law enforcement under the GDPR
   The GDPR is known for its strict enforcement system. Administrative sanctions may be imposed by the supervisory authority in an amount not exceeding: €20 million; or 4% of annual global turnover, whichever is higher. Article 83 of the GDPR states that administrative fines must be effective, proportionate, and dissuasive;
b. Law Enforcement under the PDP Act
   The PDP Act provides for both administrative and criminal sanctions. Administrative sanctions include: written warnings, temporary suspension of activities, deletion of personal data, and administrative fines. Criminal sanctions include imprisonment and fines for the illegal collection, disclosure, or falsification of personal data. According to Article 67(2), anyone who intentionally and unlawfully discloses personal information that does not belong to them may face criminal charges;
c. Comparative Effectiveness of Laws
   1) Penalty Severity: GDPR penalties are more severe and internationally recognized, particularly for multinational companies. The PDP Law includes penalties, although these are less effective as a deterrent compared to GDPR penalties.
   2) Enforcement Experience: Law enforcement agencies in the EU have gained extensive experience in enforcing data protection rules and investigating cross-border cases. In Indonesia, enforcement agencies are still relatively new and do not yet have adequate enforcement capabilities.

Cross-Border Enforcement: The GDPR incorporates an advanced cooperation framework involving supervisory authorities under the consistency mechanism and the EDPB. The PDP Law has not yet established a similar international enforcement cooperation framework. To test whether the textual equivalence between the two regimes also holds in practice, Table 2 compares the PDP Law and the GDPR on data subject rights, controller obligations, and enforcement mechanisms, and pairs each aspect with concrete implementation evidence.

Table 2. Comparison of Normative Equivalence and Operational Effectiveness: PDP Law and GDPR

Aspect	PDP Law	GDPR	Implementation evidence	Effectiveness assessment
Data subject rights	Arts. 5–15: information, access, rectification, erasure, withdrawal of consent, restriction, compensation.	Arts. 12–23, with a one-month response deadline and no fee (Art. 12), recipient notification (Art. 19), and remedies in Arts. 77–82.	GDPR: transparency failures were sanctioned separately in the TikTok case (EUR 45 million of the EUR 530 million fine) (CMS 2026). Indonesia: the 2026 civil claim over credit checks on contract workers without consent is still pending (Rajah & Tann Asia 2026b).	Norms are largely equivalent. The GDPR is *enforceable* (complaint route, sanction, judicial remedy); the PDP Law is still closer to *declaratory* because the body that receives complaints is not yet operating.
Controller obligations	Art. 35 (security, outcome-based wording), Art. 46 (breach notification within 3×24 hours), DPIA and DPO provisions. GR 33/2026 now adds operational detail (HLC 2026).	Art. 24 (accountability), Art. 30 (records), Art. 33 (72-hour notification), Art. 35 (DPIA), Arts. 37–39 (DPO).	Indonesia: a constitutional challenge to Art. 20(2)(a) on consent was rejected in 2025 on the ground that technical requirements belong in implementing regulations (Rajah & Tann Asia 2026b). GDPR: compliance can be verified through documentation and audits by the authority.	Notification deadlines are comparable, so the gap lies in *demonstrability*: the GDPR requires proof of compliance, while the PDP Law depended on implementing rules that only appeared in July 2026.
Enforcement mechanism	Art. 57 (administrative sanctions, fines up to 2% of annual revenue) and Arts. 65–73 (criminal). The supervisory agency was still at draft stage in February 2026 (Rajah & Tann Asia 2026b).	Art. 83 (fines up to EUR 20 million or 4% of worldwide turnover), Art. 58 (corrective powers), consistency mechanism through the EDPB.	GDPR: Meta, EUR 1.2 billion (May 2023); TikTok, EUR 530 million (May 2025), including an order to suspend unlawful transfers within six months (CMS 2026). Indonesia: at least 23 criminal, 7 civil, and 6 constitutional cases by March 2026, but courts applied the PDP Law mainly as an alternative basis, relying primarily on the ITE Law (Rajah & Tann Asia 2026b).	Sanction ranges are comparable, but deterrence differs. The GDPR enforces through a specialized authority; the PDP Law is enforced through general courts and a secondary role next to other statutes.

Source: Compiled by the Author (2026)

Legal Implications of the Discrepancies Between the PDP Act and the GDPR for the Protection of Personal Data in Relation to Cross-Border Data Transfers

Advances in information technology and the globalization of the digital economy have made the cross-border exchange of personal data more common. Digital business transactions require an efficient personal data protection system, especially when such transactions involve international data transfers (Saluste, 2025). On an international scale, the European Union's General Data Protection Regulation (GDPR) serves as the primary benchmark for personal data protection, as it establishes rules governing the transfer of personal data to third countries.

The Indonesian government enacted Law No. 27 of 2022 on Personal Data Protection (PDP Law) as the legal framework for personal data protection in Indonesia. Although there are some similarities between the PDP Law and the principles of the GDPR, there are still significant gaps in the regulation and enforcement of the two. These gaps result in differing legal consequences, particularly regarding legal certainty, data subjects' rights, and cross-border data transfers.

The provisions on data transfers under the GDPR can be found in Articles 44–50. According to the GDPR, the main rule is that data transfers to countries outside the EU must be made on the condition that those countries provide adequate data protection. According to Article 45 of the GDPR, "if the Commission has decided that a third country ensures an adequate level of protection, personal data may be transferred to that third country or to an international organization". In addition to an adequate decision-making process, the GDPR also recognizes the following:

1. Standard Contractual Clauses (SCCs);
2. Binding Corporate Rules (BCRs);
3. Codes of Conduct and Certification Schemes; and
4. Explicit Consent from Data Subjects

Voigt & Bussche (2021) state that restrictions on cross-border data transfers aim to prevent a lowering of personal data protection standards in the event of a transfer to another jurisdiction. Christopher Kuner also notes that cross-border data transfers have legal implications due to differences in legal systems and data protection standards between countries.

Article 56 sets forth the rules regarding cross-border transfers of personal data under the Personal Data Protection Act. Under Article 56, a personal data controller will be permitted to transfer personal data to a location outside Indonesia provided that:

a) there is an equivalent or higher level of personal data protection in the other country; or
b) there is adequate protection of personal data; or
c) the data subject has given consent

Article 56(1) of the PDP Law states: This provision clearly indicates that the adequacy approach, as set forth in the GDPR, has been implemented. However, details regarding the adequacy assessment process, standards, and procedures for supervising data transfers have not yet been provided.

The concept of "adequacy" in Article 45 of the GDPR cannot be interpreted solely based on the text, as the European Union has developed interpretive standards through the case law of the Court of Justice of the European Union (CJEU), specifically the "essentially equivalent" doctrine, which affirms that a third country need not have laws identical to the GDPR, but must provide a level of protection that is substantially equivalent, including in terms of institutional capacity to oversee and enforce it. It is this doctrine that formed the basis for the invalidation of the two previous U.S. EU data transfer frameworks, as the absence of independent supervisory authorities and effective redress mechanisms on the part of the recipient was deemed to negate substantive equivalence, even though there were textual commitments to data protection.

If this interpretive standard is applied to Article 56 of the PDP Law, then the phrase "a level of personal data protection that is equivalent to or higher than" is not sufficiently met merely by textual similarities between articles (as outlined in the previous section), but rather requires: (i) an authority explicitly designated to conduct adequacy assessments, (ii) a published assessment methodology, and (iii) a list of jurisdictions that have been declared equivalent. The absence of these three procedural elements in the PDP Law indicates that Indonesia is at the stage of

DOI: 10.58824/arjis.v5i3.648

"adequacy by aspiration," not "adequacy by design", a gap that is, from a doctrinal perspective, more fundamental than the mere absence of implementing regulations, as it concerns the structure of authority that has not yet been established in the law itself.

Differences Between the PDP Law and the GDPR:

1. Lack of an Effective Adequacy Assessment Procedure
   Under the GDPR, the European Commission can assess the level of protection in various countries. The assessment process takes place within the framework of officially developed objective procedures. In contrast, the PDP Law contains no provisions governing: who is responsible for assessing a country's level of protection, what criteria must be used in the assessment, how the destination country is assessed, or a list of countries with equivalent protection.
2. Lack of Detailed Regulations Regarding SCCs and BCRs
   Under the GDPR, legal mechanisms such as Standard Contractual Clauses (SCCs) and Binding Corporate Rules (BCRs) are used to ensure the security of cross-border data transfers. The PDP Law has not yet provided detailed rules regarding these contractual arrangements. The lack of standard contracts could result in: inadequate legal protection, an inability to establish accountability, and a greater likelihood of international disputes.
3. Lack of Independent Supervisory Authorities
   According to Article 51 of the GDPR, there must be an independent supervisory authority for each EU member state. On the other hand, the supervisory bodies responsible for implementing the Personal Data Protection Act need to be further strengthened in terms of: independence, investigative powers, and cross-border oversight capabilities.
4. Differences in the Level of Law Enforcement
   The GDPR's reputation is based on a strong law enforcement regime involving significant administrative fines. The following excerpt from Article 83 of the GDPR states: Although the PDP Law provides for administrative and criminal sanctions, its law enforcement mechanisms are still in their early stages, so their effectiveness cannot be compared to that of the GDPR.

There are differences between the GDPR and the PDP Law that could prevent Indonesia from being recognized as an adequate jurisdiction by the European Union. If that is the case, additional procedures will be required to transfer data from the EU to Indonesia; companies will have to use Standard Contractual Clauses (SCCs), and compliance costs will be higher. This could affect foreign investment and digital cooperation.

Technical uncertainties in regulations governing cross-border personal data transfers create significant compliance challenges for organizations, particularly regarding security requirements, accountability mechanisms, and the legal basis for international data transfers (Słok-Wódkowska & Mazur, 2024). Divergent regulatory approaches across jurisdictions increase legal uncertainty, raise compliance costs, and complicate corporate decision-making concerning international data governance. Differences in personal data protection standards may also undermine the protection of data subjects when personal data are transferred to jurisdictions with lower levels of legal safeguards. Consequently, cross-border data transfer frameworks require not only clear legal rules but also interoperable regulatory standards and effective enforcement mechanisms to ensure that the level of protection afforded to personal data is not diminished after international transfer (Coche et al., 2024).

In today's global digital economy, the level of data protection is a key measure of international trust. If a country lacks adequate data protection laws, it will face: restrictions on data transfers, difficulties in digital business collaboration, and a reduction in competitive advantage within the digital economy. Therefore, the differences between the PDPL and the GDPR are strategically significant for Indonesia in the global digital economy (Prastyanti & Sharma, 2024).

The difference in the magnitude of penalties between Article 83 of the GDPR (up to €20 million or 4% of global turnover) and the administrative-criminal penalties under the PDP Law is not merely a matter of the nominal amount, but reflects a difference in the deterrence theory applied. The turnover-based formula in the GDPR is designed so that the amount of the fine is proportional to the economic scale of the offender, ensuring that the deterrent effect remains effective against both large multinational corporations and SMEs, fines that, in nominal terms, would not deter large entities, while such fines could still cripple SMEs. The PDP Law employs tiered administrative sanctions and criminal penalties with fixed penalties (Article 67(2)), which structurally lack a mechanism to adjust for the economic scale of the violator, thereby risking a disproportionately lenient deterrent effect for multinational digital platforms, yet potentially disproportionate consequences for small businesses.

Furthermore, the GDPR's consistency mechanism and one-stop-shop (under the coordination of the European Data Protection Board) reflect a harmonized, cross-jurisdictional enforcement approach, whereas the absence of an equivalent international cooperation framework in the PDP Law stems from the same issue identified in the adequacy section above: the lack of a single independent supervisory authority empowered to represent Indonesia in cross-border regulatory cooperation. Thus, the weakness of law enforcement under the PDP Act is not an isolated issue, but rather a structural consequence of the same institutional deficiency that underlies the weaknesses in the areas of data subjects' rights, controllers' obligations, and data transfers, namely, the absence of an independent supervisory body with adequate investigative and coordinating capacity.

At the normative level, the PDPL incorporates the core elements of the GDPR, particularly those related to: data subject rights, data processing principles, the responsibilities of data controllers, and adequacy-based international transfers of personal data. However, there is still room for improvement in the following areas:

1.Implementation procedures;
2.Independent supervisory bodies;
3.International agreement frameworks; and
4.Effective law enforcement.

In the context of international law, the protection of personal data requires not only legal provisions but also their effective enforcement and the government's ability to oversee compliance. Therefore, in order for Indonesia to ensure the legitimacy of international personal data transfers, it must consider the following steps:

1.Establish an independent supervisory body;
2.Develop implementing regulations for international personal data transfers;
3.Adopt international treaty standards;
4.Enhance international cooperation;
5.Strengthen digital law enforcement capabilities.

The differences between the PDP Law and the GDPR regarding the regulation of cross-border data transfers have numerous legal implications in terms of legal certainty, the protection of privacy rights, and international recognition of Indonesia's data protection mechanisms. Although the PDP Law has incorporated the fundamental principles of the GDPR into its data protection

legislation, further strengthening is still needed in terms of institutional frameworks, technical regulations, and law enforcement so that Indonesia can meet international data protection standards. Indonesia will not only be able to protect the privacy rights of its citizens but will also enhance its position in international digital economic cooperation and data transfer negotiations.

CONCLUSION.

Law of the Republic of Indonesia No. 27 of 2022 on Personal Data Protection (PDP Law) represents a significant step forward by adopting fundamental global standards regarding the rights of data subjects and the obligations of data controllers; however, its substantive effectiveness remains severely hampered by critical regulatory gaps. A comparison of these two regulations reveals crucial regulatory gaps: while the GDPR excels through independent supervisory authority, strict technical requirements, and sophisticated enforcement mechanisms, Indonesia's PDP Law remains hampered by the lack of structural and political independence of its supervisory authority, the irrational formulation of administrative fines, and the absence of a robust legal framework for cross-border data transfers. It is these inconsistencies that are hindering Indonesia's efforts to obtain an Adequacy Decision from the European Union; consequently, amid escalating domestic digital vulnerabilities and a surge in data breach cases, the PDP Law currently tends to function as a symbolic legal framework rather than an operationally autonomous law enforcement instrument. Therefore, to transform the PDP Law into a robust and effective transnational protection mechanism, Indonesia must take aggressive steps to refine implementing regulations, uphold the institutional autonomy of the supervisory authority, and enhance technical compliance capacity and public legal awareness.

To transform the Personal Data Protection Act (PDP Act) from a mere symbolic regulation into a robust law enforcement instrument that meets international standards, a crucial step that the Indonesian government must take immediately is to restructure institutional governance by establishing a fully independent personal data protection oversight agency, free from any structural or financial interference by the executive branch. Simultaneously, the government must expedite the enactment of implementing regulations (Government Regulations) that explicitly establish a rational and proportional matrix for calculating administrative fines, while also institutionalizing globally recognized transnational legal instruments such as Standard Contractual Clauses (SCCs) and Binding Corporate Rules (BCRs) to facilitate secure cross-border data transfers. Furthermore, this regulatory strengthening must be balanced with enhanced institutional capacity for law enforcement agencies and the implementation of mandatory periodic compliance audits for data controllers, particularly in critical and vulnerable sectors such as healthcare and finance, so that the Personal Data Protection Act (PDP Act) can meet the criteria for the European Union's Adequacy Decision while providing active and effective legal protection against the evolving threats to global digital privacy.

ACKNOWLEDGMENT

The authors thank their colleagues for the valuable discussions that helped sharpen the arguments in this article. The authors also appreciate the constructive comments of the anonymous reviewers.

FUNDING

This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

AUTHOR CONTRIBUTIONS STATEMENT

RKS contributed to the conceptualization, methodology, investigation, formal analysis, and writing of the original draft. HYA was responsible for data curation, validation, visualization of the comparative tables, and writing through review and editing. EL managed the project administration, and contributed to writing through review and editing. All authors have read and approved the final manuscript.

AI USAGE STATEMENT

Generative artificial intelligence technology is used to a limited extent to refine the linguistic aspects of the text, including style, grammar, and readability, without being involved in the formulation of ideas, substantive analysis, interpretation of legal norms, or the drawing of academic conclusions. Intellectual authority over the entire content of the manuscript remains with the author, who independently reviews and verifies the validity of the legal material, the accuracy of references and citations, and the consistency of the analysis and conclusions.

CONFLICT OF INTEREST

The authors declare that there are no conflicts of interest related to this research or the publication of this article.

REFERENCES

Absor, A. M. (2023). Juridical Analysis of Human Rights Protection in the Era of Digital Transformation: Perspective of Laws and Regulations. *Indonesia Media Law Review*, *2*(2). https://doi.org/10.15294/imrev.v2i2.69472

Aura, A., Priowirjanto, E. S., & Dewi, C. T. I. (2025). Privacy Protection Guarantee for Data Hacking Victims According to Indonesian Law. *Padjadjaran Journal of International Law*, *9*(1), 1–15. https://doi.org/10.23920/pjil.v8i2.1823

Cejas, O. A., Sannier, N., Abualhaija, S., Ceci, M., & Bianculli, D. (2025). *GDPR-Relevant Privacy Concerns in Mobile Apps Research: A Systematic Literature Review* (arXiv:2411.19142). arXiv. https://doi.org/10.48550/arXiv.2411.19142

Chong, A. (2026, February 25). *Cross-Border Personal Data Transfers: The Remaining Issues Following the Indonesian Constitutional Court Decision*. https://conflictoflaws.net/2026/cross-border-personal-data-transfers-the-remaining-issues-following-the-indonesian-constitutional-court-decision/

Coche, E., Kolk, A., & Ocelík, V. (2024). Unravelling cross-country regulatory intricacies of data governance: The relevance of legal insights for digitalization and international business. *Journal of International Business Policy*, *7*(1), 112–127. https://doi.org/10.1057/s42214-023-00172-1

Creswell, John W., and J. David Creswell. (2023). Research Design: Qualitative, Quantitative, and Mixed Methods Approaches. 6th ed. Thousand Oaks, CA: SAGE Publications.

Elza, P. (2025). Tinjauan Hukum Perlindungan Data Pribadi dalam Peraturan Perundang-Undangan di Indonesia. *Jurnal Ilmu Hukum*, *1*(1), 1–7.

Fachran, S., Rosadi, S. D., & Amalia, P. (2026). PROTECTION OF DATA SUBJECT RIGHTS IN THE TRANSFER OF PERSONAL DATA BETWEEN DATA CONTROLLERS IN INDONESIA: A COMPARATIVE ANALYSIS OF THE PDP LAW AND THE EU GDPR. *Awang Long Law Review*, *8*(2), 518–529. https://doi.org/10.56301/awl.v8i2.1827

Fauzy, E., & Shandy, N. A. R. (2022). Hak Atas Privasi dan Politik Hukum Undang-Undang Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi. *Lex Renaissance*, *7*(3), 445–461. https://doi.org/10.20885/JLR.vol7.iss3.art1

Kriswandaru, A. S., Pratiwi, B., & Suwardi, S. (2024). Efektivitas Kebijakan Perlindungan Data Pribadi di Indonesia: Analisis Hukum Perdata dengan Pendekatan Studi Kasus. *Hakim: Jurnal Ilmu Hukum Dan Sosial*, *2*(4), 740–756. https://doi.org/10.51903/hakim.v2i4.2157

Manurung, E. A. P., & Thalib, E. F. (2022). Tinjauan Yuridis Perlindungan Data Pribadi Berdasarkan Uu Nomor 27 Tahun 2022. *Jurnal Hukum Saraswati (JHS)*, *4*(2), 139–148.

Marelli, M. (2024). Transferring personal data to international organizations under the GDPR: An analysis of the transfer mechanisms. *International Data Privacy Law*, *14*(1), 19–36. https://doi.org/10.1093/idpl/ipad022

Nusantara, A. H. S., Umam, I. K., & Lubis, M. (2024). Jaminan Informasi dan Keamanan yang Lebih Baik: Studi Kasus BPJS Kesehatan. *NUANSA INFORMATIKA*, *18*(2), 120–127. https://doi.org/10.25134/ilkom.v18i2.202

Prastyanti, R. A., & Sharma, R. (2024). Establishing Consumer Trust Through Data Protection Law as a Competitive Advantage in Indonesia and India. *Journal of Human Rights, Culture and Legal System*, *4*(2), 354–390. https://doi.org/10.53955/jhcls.v4i2.200

Rahman, F., & Mulyani, C. K. (2025). Minimising unnecessary restrictions on cross-border data flows? Indonesia's position and challenges post personal data protection act enactment. *International Review of Law, Computers & Technology*, *39*(2), 281–300. https://doi.org/10.1080/13600869.2024.2359901

Rajah & Tann Asia (2026). PDP Law Updates: The PDP Implementing Regulation Is Out, and It Clarifies Some Key Questions Under Indonesia′ s PDP Law https://www.rajahtannasia.com/viewpoints/pdp-law-updates-the-pdp-implementing-regulation-is-out-and-it-clarifies-some-key-questions-under-indonesias-pdp-law/.

Saluste, M. (2025). Cross-Border 'Data Adequacy' Frameworks under GATS Article VII: Aligning WTO Members' Rights to Protect Personal Data with Their International Commitments. *World Trade Review*, *24*(5), 593–619. https://doi.org/10.1017/S1474745625000047

Satory, A., Febrianty, Y., Astuti, W. R. B., & Pradana, A. F. K. (2024). METODE PENELITIAN HUKUM. *Penerbit Tahta Media*. https://tahtamedia.co.id/index.php/issj/article/view/1031

Siems, Mathias. (2022). Comparative Law. 3rd ed. Cambridge: Cambridge University Press.

Simanjuntak, P. H. (2024). PERLINDUNGAN HUKUM TERHADAP DATA PRIBADI PADA ERA DIGITAL DI INDONESIA: STUDI UNDANG - UNDANG PERLINDUNGAN DATA PRIBADI DAN GENERAL DATA PROTECTION REGULATION (GDPR). *Esensi Hukum*, *6*(2), 105–124. https://doi.org/10.35586/esensihukum.v6i2.412

Słok-Wódkowska, M., & Mazur, J. (2024). Between commodification and data protection: Regulatory models governing cross-border information transfers in regional trade agreements. *Leiden Journal of International Law*, *37*(1), 111–138. https://doi.org/10.1017/S092215652300050X

Voigt, P., & Bussche, A. von dem. (2021). *The EU General Data Protection Regulation (GDPR): A practical guide*. Springer International Publishing.

Wibowo, A., Alawiyah, W., & Azriadi. (2024). The importance of personal data protection in Indonesia's economic development. *Cogent Social Sciences*, *10*(1), 2306751. https://doi.org/10.1080/23311886.2024.2306751