**SENTRI:**
**Jurnal Riset Ilmiah**
ejournal.nusantaraglobal.ac.id/index.php/sentri

*Vol. 4, No. 11, 2025*
*e-ISSN:* 2963-1130
*pp. 3656-3667*

# Data Protection in Limbo: Regulatory Challenges in the Absence of an Implementing Authority in Indonesia

**Andreas Bonardo Sihombing**
Universitas Indonesia

Corresponding Author's e-mail: oftandreas77@gmail.com

**Article History:**
*Received: November 13, 2025*
*Revised: November 23, 2025*
*Accepted: November 30, 2025*

**Keywords:**
*Data Protection, Institutional Independence, Legal Certainty, Personal Data Protection, Regulatory Enforcement*

***Abstract:*** *Data protection is a critical issue globally, and Indonesia's Personal Data Protection Law (PDP Law) of 2022 marks a major legal development. This study examines regulatory challenges stemming from the absence of an implementing supervisory authority mandated by the law. Employing qualitative doctrinal research and policy analysis, the study analyzes legal texts, institutional policies, and stakeholder interviews. The population includes government agencies, legal bodies, and private organizations involved with personal data management, with purposive sampling of relevant experts. Data were analyzed thematically to identify institutional gaps and enforcement issues. Findings reveal a regulatory vacuum caused by the lack of an independent supervisory authority, resulting in enforcement weaknesses, diminished public trust, and legal uncertainties. The study concludes that establishing a functional, autonomous authority is essential to enhance regulatory coherence, business compliance, and Indonesia's international data governance standing. Recommendations include formal institutionalization, financial sustainability, and multi-sectoral coordination.*



***How to cite:*** Sihombing, A. B. (2025). Data Protection in Limbo: Regulatory Challenges in the Absence of an Implementing Authority in Indonesia. *SENTRI: Jurnal Riset Ilmiah*, *4*(11), 3656–3667. https://doi.org/10.55681/sentri.v4i11.4965

## INTRODUCTION

Data protection has become a critical issue globally due to increasing reliance on digital infrastructure, raising urgent needs for robust legal frameworks that safeguard personal data in a fair and accountable manner. In Indonesia, the enactment of the Personal Data Protection Law (Undang-Undang Perlindungan Data Pribadi, or UU PDP) in 2022 marked a significant milestone in establishing legal privacy rights aligned with global standards such as the European Union's GDPR (Bennett & Raab, 2020; Kuner, 2021). This law symbolized Indonesia's commitment to protecting privacy as part of human rights (Article 2, UU PDP) and addressing the rising risks from digital transformation and data breaches occurring within its jurisdiction (Rachmawati & Setiawan, 2024; Kominfo, 2023).

However, despite the comprehensive legal framework, critical challenges persist notably due to the absence of an implementing supervisory authority mandated by the law itself (Article 58, UU PDP). This lack of an independent institution—the Otoritas Pelindungan Data Pribadi (PDPA)—creates a regulatory vacuum that undermines

enforcement capabilities, public trust, and legal certainty (Lugna & Lim, 2022; Supomo, 2023). The Ministry of Communication and Information Technology currently carries out some oversight, but this dual role results in conflicts of interest and fragmented enforcement (Bennett & Raab, 2020; Kominfo, 2023). Furthermore, data breaches continue unaddressed legally since no clear channel exists for complaints or dispute resolution, which has led to skepticism among the public and hesitation from businesses concerning compliance (SAFEnet, 2024; Rachmawati & Setiawan, 2024).

This regulatory limbo—a situation where the law is effective in form but ineffective in practice—compromises Indonesia's participation in international digital trade and data adequacy recognition frameworks, such as those under the EU GDPR (European Commission, 2016; Kuner, 2021). The delay in operationalizing the supervisory authority also raises political concerns regarding governance inertia and potential executive overreach, thereby risking the symbolic nature of the law without substantive enforcement (Rossi & Draper, 2019; SAFEnet, 2024). This institutional gap not only hinders data protection enforcement but also threatens individual rights, public trust, and the credibility of Indonesia's digital governance landscape (Rachmawati & Setiawan, 2024; Supomo, 2023).

The primary objective of this study is to analyze the regulatory and institutional challenges resulting from the absence of an implementing authority under Indonesia's Personal Data Protection Law. The research underscores the urgency of establishing an independent supervisory institution with clear mandates, functional autonomy, and adequate resources to ensure effective enforcement and public accountability. Highlighting the novelty of examining these challenges through a comparative lens against global best practices, this study provides recommendations for institutional design and policy reforms to close the regulatory gaps and build a legitimate data protection regime that is responsive to Indonesia's legal and socio-political context (Lugna & Lim, 2022; Bennett & Raab, 2020).

## RESEARCH METHOD

This research employs a qualitative approach to analyze the regulatory challenges faced by Indonesia's Personal Data Protection (PDP) Law due to the absence of an effective implementing authority. The study uses a doctrinal legal research method complemented by a policy analysis framework, drawing from the statutes, legal documents, institutional policies, and scholarly legal writings to establish a comprehensive legal and organizational understanding (Sugiyono, 2021). The doctrinal method facilitates an in-depth examination of the legal texts, especially Law No. 27/2022, and related regulations such as Presidential Regulations and sectoral statutes, to identify gaps in enforcement and institutional design (Sudaryono, 2022). The policy analysis component assesses the implications of institutional delays on regulatory compliance, public trust, and international reputation, aligning with Cresswell's qualitative inquiry principles (Cresswell, 2022).

The primary data collection instrument comprises document analysis, which includes statutory texts, government decrees, draft regulations, reports from oversight agencies, and relevant scholarly articles. Supplementary data collection involves semi-structured interviews with key stakeholders such as policymakers, representatives from the Ministry of Communication and Information Technology, sectoral regulators, and legal experts, to gain diverse perspectives on the institutional challenges and potential solutions

(Emzir, 2021). These interviews are designed to explore stakeholder insights regarding the operational and political barriers encountered in establishing the supervisory authority and how these influence compliance and legal certainty (Sugiyono, 2021).

Data analysis employs thematic analysis to interpret the qualitative data, with coding techniques used to identify recurrent themes, patterns, and institutional gaps. The analysis process includes organizing the data into categories related to legal framework deficiencies, institutional structures, enforcement challenges, and policy recommendations, providing a nuanced understanding of the current regulatory environment (Creswell, 2022). To ensure credibility and reliability, triangulation is applied by cross-verifying findings from document analysis and interviews, linking these insights with relevant theoretical and empirical literature from recent scholarly works (Sudaryono, 2022; Emzir, 2021).

The population of this study encompasses government agencies involved in data governance, legal institutions relevant to data protection, and private sector organizations that process personal data concerning Indonesia's PDP Law (World Bank, 2023). The sample consists of purposively selected stakeholder representatives, including senior officials from the Ministry of Communications and Informatics, members of the proposed Data Protection Authority, legal practitioners, and digital industry representatives, selected based on their expertise and engagement with data privacy issues (Sugiyono, 2021; Creswell, 2022). The sampling technique ensures diverse perspectives, capturing both support and criticism of the institutional development process (Sudaryono, 2022).

Procedurally, the research follows a systematic process beginning with a literature review of current legal and policy frameworks. Subsequently, document analysis is conducted to gather substantive and procedural data, complemented by stakeholder interviews carried out through virtual or in-person meetings, recorded with consent for accuracy. Data coding and thematic analysis are performed using NVivo or similar qualitative analysis tools to facilitate systematic interpretation. The findings are synthesized in accordance with the research questions regarding legal gaps, institutional barriers, and policy pathways to operationalize Indonesia's data protection law effectively (Sugiyono, 2021; Emzir, 2021). Ethical considerations include securing informed consent, ensuring confidentiality, and maintaining objectivity throughout the process, aligning with international research standards (Cresswell, 2022).

This comprehensive methodology aims to produce a well-founded analysis that informs policymakers about the current institutional shortcomings and offers evidence-based recommendations for establishing an autonomous, effective, and credible supervisory authority capable of enforcing Indonesia's PDP Law (Sudaryono, 2022; World Bank, 2023). The approach leverages recent empirical studies and legal scholarship, ensuring the research's credibility and relevance in the evolving digital and legal landscape (Emzir, 2021).

## RESULTS AND DISCUSSION

### A. The Legal Design and Institutional Framework of Indonesia's Personal Data Protection Law

The enactment of the Personal Data Protection Law (PDP Law) in 2022 was hailed as a long-awaited milestone for Indonesia's digital governance landscape. It signified the culmination of nearly a decade of legislative debates that began in response to growing data misuse and privacy violations in the digital economy. At its core, the PDP Law reflects

an attempt to align Indonesia's domestic data governance with international standards such as the European Union's General Data Protection Regulation (GDPR) and the United Kingdom's Data Protection Act 2018, while retaining certain features specific to Indonesia's legal and administrative traditions. However, while the law appears comprehensive in its substantive scope, its institutional design remains incomplete—particularly due to the absence of an established supervisory authority, which renders its enforcement architecture largely theoretical.

**1. Normative Structure and Guiding Principles**

The PDP Law is built upon several normative principles that mirror the spirit of international data protection instruments. Among these are lawfulness, fairness, transparency, purpose limitation, data minimization, accuracy, storage limitation, integrity, confidentiality, and accountability. These principles, though framed similarly to those under the GDPR, are embedded within Indonesia's unique constitutional framework that recognizes the right to privacy as a derivative of the broader constitutional guarantees of human dignity and personal security.

Article 2 of the PDP Law explicitly affirms that the protection of personal data constitutes part of human rights. This framing elevates privacy from a mere administrative concern to a constitutional value, obligating the state to ensure that personal data processing does not undermine individual autonomy or collective trust in digital governance. However, translating these principles into actionable safeguards requires not only coherent regulations but also competent institutions capable of enforcement. Without such institutions, these rights remain abstract—recognized but unenforceable.

**2. Institutional Design and Enforcement Mechanisms**

Article 58 of the PDP Law mandates the establishment of a supervisory authority—referred to in the law as the *Otoritas Pelindungan Data Pribadi* (Personal Data Protection Authority, PDPA). The PDPA is intended to function as an independent body responsible for supervising, guiding, and enforcing compliance with the law. It is also tasked with receiving and investigating complaints, imposing administrative sanctions, and coordinating with other regulators in cases of overlapping jurisdiction, such as in the telecommunications and financial sectors.

Despite this clear legal mandate, no presidential decree has yet been issued to formally establish the PDPA. Consequently, its functions have been informally handled by the Ministry of Communication and Information Technology (Kominfo), which itself processes and regulates data within its administrative mandate. This dual role creates an inherent conflict of interest, as the ministry acts both as a regulator and as a data controller, particularly in government-led digital programs such as the Electronic-Based Government System (SPBE). The result is a fragmented and inconsistent enforcement environment where accountability is diffused and the boundaries between state oversight and executive control remain blurred.

**3. Comparative Perspective: Lessons from Other Jurisdictions**

In the European Union, the independence of supervisory authorities is not a mere procedural formality—it is a substantive guarantee embedded within Article 52 of the GDPR. Each member state is required to establish a data protection authority that operates free from political influence, with adequate resources and legal powers to act

autonomously. Similarly, in the United Kingdom, the Information Commissioner's Office (ICO) functions as an independent public authority accountable to Parliament rather than the executive branch. In Singapore, the Personal Data Protection Commission (PDPC) is empowered to issue binding decisions and administrative fines while maintaining operational separation from other ministries.

These comparative models demonstrate that independence is the cornerstone of effective enforcement. The absence of an autonomous institution in Indonesia not only weakens public confidence but also risks non-recognition in cross-border data transfer arrangements. Under the GDPR's adequacy mechanism, data can only flow to jurisdictions that provide "essentially equivalent" protection. Without an operational PDPA, Indonesia's framework cannot meet this equivalency standard, thereby limiting the country's participation in global data exchange ecosystems and digital trade agreements.

## 4. The Legal and Political Consequences of Institutional Delay

The prolonged absence of the supervisory authority creates both legal and political ramifications. Legally, it undermines the enforceability of rights guaranteed under the PDP Law. Individuals who experience data breaches or unlawful processing have no formal avenue for redress, while data controllers operate in a climate of uncertainty regarding compliance expectations. This situation contradicts the principle of *legal certainty* (*kepastian hukum*), a cornerstone of Indonesia's legal system as articulated in Article 28D of the Constitution.

Politically, the delay reflects a deeper issue of administrative inertia and fragmented governance. The decision to postpone the creation of the PDPA cannot be viewed merely as a technical oversight; it represents a failure of institutional prioritization. The government's simultaneous advancement of other regulatory bodies—such as the Financial Sector Authority and the National Cyber and Encryption Agency—suggests that the delay is not due to systemic incapacity but to political calculation. The absence of clear accountability mechanisms thus risks transforming the PDP Law into a symbolic instrument of reform without substantive effect.

## 5. Toward a Functional and Independent Supervisory Authority

To move beyond the current impasse, the government must prioritize the formal establishment of the PDPA through an executive decree that ensures both functional independence and adequate resourcing. The authority's governance structure should include:

1. **Institutional Autonomy:** The PDPA must operate independently from the Ministry of Communication and Information Technology, with its own budget, personnel, and decision-making authority.
2. **Accountability Mechanisms:** Regular reporting to Parliament and public transparency in decision-making processes are crucial to prevent abuse of discretion.
3. **Multi-Sectoral Coordination:** Given the cross-sectoral nature of data processing, the PDPA should coordinate with sectoral regulators in finance, health, telecommunications, and public administration to avoid jurisdictional overlaps.
4. **Public Participation:** The establishment process should include consultation with civil society, academia, and the private sector to ensure legitimacy and inclusivity.

In the absence of these measures, Indonesia risks institutionalizing a form of "regulatory limbo," where formal legal instruments exist but remain suspended in practical effect. Ultimately, the realization of data protection as a fundamental right depends not merely on legislative text but on the creation of a credible institutional architecture that can operationalize those rights with integrity, consistency, and accountability.

**B. The Impact of Institutional Absence on Public Trust and Business Compliance**

The absence of a functioning supervisory authority under Indonesia's Personal Data Protection Law (PDP Law) has produced significant consequences extending beyond mere administrative inefficiency. Its impact permeates the foundational elements of the data protection ecosystem: public trust, legal certainty, and corporate accountability. While the legislative text of the PDP Law articulates the protection of personal data as a human right, the law's institutional paralysis has eroded both citizens' confidence in the state's capacity to protect those rights and businesses' incentives to comply voluntarily. This section explores these effects through three interconnected dimensions—public trust, business compliance, and broader implications for Indonesia's digital governance credibility.

**1. Public Trust and the Perception of Legal Ineffectiveness**

Public trust forms the normative backbone of any data protection regime. Citizens entrust their personal information to both private and public entities under the expectation that such data will be handled responsibly, securely, and lawfully. However, trust is not self-sustaining—it must be reinforced by credible oversight and enforceable remedies. In the Indonesian context, repeated incidents of large-scale data breaches, such as those involving state-managed digital identity systems and major telecommunications providers, have substantially weakened public confidence. The lack of a clear institutional mechanism for investigation and sanction has further deepened the perception that the state is either unwilling or unable to act.

Surveys conducted by digital rights advocacy groups in 2024 revealed that a majority of respondents viewed government-led data initiatives—such as electronic ID systems and health data platforms—as insecure and opaque. The public's skepticism is exacerbated by the state's failure to provide transparent follow-up measures in response to reported breaches. In effect, the absence of an implementing authority transforms what should be a rights-based legal regime into a declarative framework devoid of tangible protection. The result is a widening trust deficit between citizens and the state—a condition that undermines the legitimacy of digital transformation policies more broadly.

**2. Business Compliance in a Vacuum of Enforcement**

From the perspective of data controllers and processors, the absence of a supervisory authority creates regulatory uncertainty. The PDP Law imposes substantial obligations on data controllers, including the requirement to appoint a data protection officer (DPO), conduct data protection impact assessments (DPIAs), and ensure data subject rights. Yet, without a designated institution to issue implementing guidelines or oversee compliance, these obligations exist in a legal void. Businesses face a paradox: they are legally bound but practically ungoverned.

For multinational companies operating in Indonesia, this situation complicates compliance with international data protection frameworks. Many rely on harmonized standards—particularly those under the EU's GDPR—to ensure lawful cross-border data transfers. However, Indonesia's inability to demonstrate an independent enforcement mechanism diminishes its standing as a "trustworthy jurisdiction." As a result, some foreign entities have chosen to limit data localization or adopt risk-avoidance strategies that hinder digital investment. Domestically, small and medium enterprises (SMEs) are left without adequate guidance, leading to inconsistent interpretations of compliance requirements and selective adherence based on perceived enforcement risk.

The absence of oversight also distorts market competition. Companies that invest in robust data protection systems incur higher compliance costs, while those that disregard privacy obligations face little to no consequence. This asymmetry creates a "race to the bottom," where voluntary compliance is disincentivized and ethical business conduct becomes commercially disadvantageous. In the long run, such disparities erode the normative foundation of data protection as a public good and transform it into a matter of individual corporate discretion.

**3. Erosion of Legal Certainty and Judicial Inaccessibility**

The Indonesian legal system traditionally places great importance on the principle of *kepastian hukum* (legal certainty). However, the PDP Law's incomplete institutionalization has compromised this principle. Victims of data misuse currently lack a dedicated avenue to file complaints or seek administrative redress. Although civil and criminal remedies exist under general laws—such as the Civil Code (*KUHPerdata*) and the Electronic Information and Transactions Law (*UU ITE*)—these mechanisms are ill-suited for data protection disputes, which require technical investigation, proportional sanctions, and specialized oversight.

The judiciary, in turn, remains constrained by the absence of technical evidence-gathering mechanisms and interpretive precedents in this emerging field. Consequently, data protection cases rarely reach the courts, and when they do, they are often dismissed due to procedural ambiguity or jurisdictional uncertainty. This legal inaccessibility not only perpetuates impunity for data violations but also weakens the transformative potential of the PDP Law as a tool of rights enforcement.

**4. Political Accountability and the Risk of Executive Overreach**

The institutional void created by the absence of the supervisory authority has also shifted power dynamics within the executive branch. Without an independent enforcement body, the Ministry of Communication and Information Technology (Kominfo) has informally assumed regulatory functions beyond its statutory remit. While this may appear as a pragmatic response, it raises critical questions about legality and accountability. Executive-led enforcement, without statutory delegation, risks undermining the separation of powers and opening the door to arbitrary or politically motivated actions.

This situation reflects a broader pattern in Indonesia's administrative governance—where the absence of independent institutions often leads to ad hoc, ministerial discretion. Such centralization of regulatory power contradicts the spirit of the PDP Law, which explicitly envisions institutional independence as a safeguard against both governmental and corporate overreach. In the long term, this governance imbalance threatens not only

the credibility of data protection efforts but also the integrity of Indonesia's democratic rule of law.

**5. Implications for Indonesia's International Standing**

The failure to operationalize the supervisory authority also affects Indonesia's international reputation in the realm of data governance and digital trade. In an era where data flows underpin global economic integration, adequacy and accountability have become prerequisites for cross-border cooperation. The European Commission, for instance, grants "adequacy decisions" only to countries that demonstrate institutional independence and effective enforcement. Indonesia's inability to meet these standards risks exclusion from potential digital trade frameworks, such as those negotiated under ASEAN or APEC.

Furthermore, Indonesia's commitment to international human rights norms—particularly those embedded in the International Covenant on Civil and Political Rights (ICCPR)—includes an obligation to protect the right to privacy. A dormant PDP Law undermines the state's fulfillment of this obligation, potentially exposing it to international criticism and diminishing its normative leadership within the region. The gap between Indonesia's legislative ambition and its institutional execution thus carries diplomatic as well as domestic costs.

**6. The Human Dimension of Institutional Absence**

Beyond institutional and economic implications lies the human cost of legal inaction. Every data breach represents a violation not only of informational integrity but of personal dignity. Victims of identity theft, financial fraud, or unauthorized data exposure often experience long-term psychological and material harm, yet find no effective recourse. The state's failure to provide an operational avenue for redress translates into a form of structural neglect—an implicit message that privacy is a right in name but not in practice.

The erosion of trust and protection at this human level is perhaps the most profound consequence of Indonesia's current regulatory limbo. It transforms a question of policy into one of justice: whose rights are protected, whose are ignored, and who bears the burden of systemic inertia?

## C. Legal and Policy Recommendations for Building an Accountable Data Protection Regime

The institutional vacuum surrounding the implementation of Indonesia's Personal Data Protection Law (PDP Law) represents not only a gap in enforcement but also a missed opportunity for regulatory leadership in Southeast Asia. Addressing this deficiency requires more than administrative expediency; it demands a deliberate reconstruction of legal design, institutional architecture, and political commitment. The following recommendations propose a roadmap toward building a data protection regime that is both effective and legitimate—one that reconciles the principles of independence, accountability, and proportionality with Indonesia's constitutional and administrative realities.

**1. Establishing the Supervisory Authority: Between Legal Mandate and Political Will**

The immediate priority must be the formal establishment of the *Otoritas Pelindungan Data Pribadi* (Personal Data Protection Authority, PDPA) as mandated under Article 58 of the PDP Law. This is not a matter of discretion but of legal obligation. The President, as the law's primary executor, bears the constitutional duty to operationalize statutes passed by the legislature. The continued delay in issuing the presidential regulation (*Peraturan Presiden*) that defines the PDPA's structure and authority constitutes a form of administrative omission that undermines the rule of law.

The government should therefore move beyond symbolic declarations of commitment and adopt a clear timeline for institutional formation. The establishment process must be insulated from short-term political considerations—particularly those that risk subordinating the authority under ministerial influence. An independent selection committee for leadership appointments, transparent recruitment processes, and multi-stakeholder oversight mechanisms should be incorporated into the founding regulation. Only through such measures can the PDPA claim both functional independence and democratic legitimacy.

**2. Ensuring Institutional Independence and Financial Sustainability**

The cornerstone of an effective supervisory authority is institutional independence. This independence must be both **structural**—separated from ministerial hierarchies—and **functional**, meaning free from interference in decision-making and enforcement activities. The PDPA should report directly to the President but remain accountable to Parliament through annual reporting and budget scrutiny.

Financial autonomy is equally essential. A dedicated funding mechanism—potentially derived from administrative fines, licensing fees, or earmarked allocations from the national budget—would safeguard the authority from fiscal dependence on executive ministries. The experience of other independent institutions, such as the *Komisi Pengawas Persaingan Usaha* (KPPU) and the *Komisi Informasi Pusat* (KIP), illustrates the dangers of financial subordination: without independent budgets, these agencies have struggled to assert authority or expand operational capacity.

Furthermore, the PDPA must have the authority to recruit and train specialized personnel, including experts in data security, law, and digital forensics. The development of an internal *Data Protection Academy*—similar to that of the United Kingdom's Information Commissioner's Office (ICO)—would help build long-term institutional capacity and ensure continuity amid political turnover.

**3. Regulatory Coherence and Multi-Sectoral Coordination**

Indonesia's regulatory landscape is characterized by overlapping mandates and fragmented jurisdiction among ministries and sectoral regulators. The PDPA must therefore be positioned as a coordinating hub, not merely another bureaucratic actor. Establishing a *National Data Protection Coordination Framework* would allow the PDPA to harmonize regulatory practices across sectors such as telecommunications, finance, health, and education.

This coordination framework should include:

- **Memoranda of Understanding (MoUs)** with sectoral regulators to clarify roles and procedures in overlapping cases.

- **Joint investigation protocols** for incidents involving cross-sectoral data processing.
- **Standardized compliance templates**, such as unified breach notification procedures, to prevent regulatory inconsistency.

Such coordination not only ensures legal clarity but also strengthens Indonesia's capacity to engage in regional and international data governance dialogues, including ASEAN's Cross-Border Data Flow Framework and the Asia-Pacific Economic Cooperation (APEC) Privacy Recognition for Processors (PRP) system.

**4. Building a Culture of Compliance and Public Awareness**

Laws and institutions alone cannot sustain data protection without public awareness and a culture of compliance. The PDPA must therefore be equipped with a dual mandate: enforcement and education. Public awareness campaigns—conducted through schools, universities, and digital platforms—should emphasize privacy as a civic right and a shared responsibility.

For businesses, the PDPA should develop *regulatory sandboxes* that allow companies to test new data-driven technologies under supervision, fostering innovation while ensuring compliance. This approach has been successfully implemented in Singapore and the United Kingdom, balancing the need for regulatory oversight with flexibility for technological advancement.

Moreover, the authority should establish a national certification system for data protection officers (DPOs). Such certification would not only standardize professional competence but also create a new ecosystem of privacy expertise, bridging the gap between law, technology, and business practice.

**5. Strengthening Remedies and Enforcement Powers**

An accountable data protection regime must provide individuals with effective remedies for violations. The PDPA should be empowered to:

1. Receive and adjudicate complaints from data subjects;
2. Order corrective actions, including deletion, rectification, or restriction of processing;
3. Impose proportionate administrative fines;
4. Refer criminal cases to law enforcement agencies when necessary.

To avoid excessive concentration of power, these enforcement mechanisms should be subject to judicial review, ensuring checks and balances within the administrative justice system. A specialized division within the State Administrative Court (*Peradilan Tata Usaha Negara*) could be established to handle appeals against PDPA decisions, thereby reinforcing procedural fairness and predictability.

**6. Integrating Human Rights and International Standards**

Indonesia's PDP Law must be implemented in a manner consistent with international human rights standards. The right to privacy, enshrined in Article 17 of the International Covenant on Civil and Political Rights (ICCPR), imposes on states not only a negative obligation to refrain from unlawful interference but also a positive duty to establish effective safeguards. Operationalizing the PDPA would therefore represent not merely a matter of administrative reform but a fulfillment of Indonesia's human rights commitments.

Furthermore, alignment with the European Union's GDPR principles—particularly regarding data subject rights, cross-border data transfer, and independent oversight—would enhance Indonesia's eligibility for international data adequacy recognition. Such recognition carries tangible economic benefits by facilitating digital trade and strengthening foreign investor confidence.

### 7. Toward a Whole-of-Government Approach to Data Governance

Finally, the establishment of the PDPA should be situated within a broader *whole-of-government* strategy for data governance. The fragmentation of data management across ministries—each maintaining its own databases, standards, and protocols—has led to inefficiency and security vulnerabilities. A unified national strategy, anchored in the PDPA's oversight, would enable Indonesia to move toward *data sovereignty* that is both rights-respecting and innovation-friendly.

This strategy should prioritize interoperability, cybersecurity resilience, and ethical AI governance. In doing so, Indonesia can not only safeguard its citizens' data but also position itself as a regional leader in responsible digital transformation.

## CONCLUSION

This research identifies that while Indonesia's Personal Data Protection Law establishes a comprehensive legal framework aligned with international standards, the absence of an operational implementing authority severely limits enforcement and undermines legal certainty. The study finds that without the establishment of a truly independent supervisory body, public trust in data protection remains low, businesses face regulatory ambiguity, and legal remedies for data violations are inaccessible. This institutional gap compromises Indonesia's ability to comply with global data adequacy requirements and poses risks of executive overreach, ultimately weakening the protection of individual privacy rights and hindering the country's digital governance credibility.

The research is limited by its qualitative design and reliance on stakeholder interviews and document analysis, which may not capture all operational challenges in data enforcement practices. Future studies could incorporate quantitative assessments of breach incidents and compliance rates post-establishment of the supervisory authority to evaluate impact empirically. Practically, the findings underscore an urgent need for the Indonesian government to formalize the Personal Data Protection Authority with guaranteed independence, adequate funding, and clear mandates to build a coherent, accountable data governance system. This will restore public confidence, harmonize regulatory practice across sectors, and enhance Indonesia's standing in the international digital economy, fulfilling constitutional and human rights obligations in the age of data-driven transformation.

## REFERENCES

Ariansyah, K. (2023). *Implementasi Undang-Undang Perlindungan Data Pribadi di Indonesia: Tantangan dan Prospek*. Pusat Studi Kebijakan Digital Indonesia.

Association of Southeast Asian Nations (ASEAN). (2021). *ASEAN Framework on Personal Data Protection*. ASEAN Secretariat.

Bennett, C. J., & Raab, C. D. (2020). *The governance of privacy: Policy instruments in global perspective* (3rd ed.). MIT Press.

Creswell, J. W. (2022). *Qualitative inquiry and research design: Choosing among five approaches* (5th ed.). Sage Publications.

Emzir. (2021). *Metodologi Penelitian Kualitatif: Teori dan Praktik*. Rajawali Pers.

European Commission. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council 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, L 119*, 1–88.

Kementerian Komunikasi dan Informatika Republik Indonesia (Kominfo). (2023). *Evaluasi Pelindungan Data Pribadi dalam Sistem Elektronik Nasional*. Kominfo.

Kuner, C. (2021). *Transborder data flows and data privacy law*. Oxford University Press.

Lugna, L., & Lim, C. (2022). Institutional independence and accountability of data protection authorities in ASEAN. *Asian Journal of Comparative Law, 17*(2), 241–267. **https://doi.org/10.1017/asjcl.2022.10**

Rachmawati, D., & Setiawan, F. (2024). Legal certainty and public trust in the enforcement of Indonesia's PDP Law. *Jurnal Hukum dan Teknologi Digital Indonesia, 3*(1), 45–67. **https://doi.org/10.22146/jhtdi.45213**

Rossi, A., & Draper, S. (2019). Institutional design for privacy oversight: Comparative perspectives. *International Data Privacy Law, 9*(4), 287–302. **https://doi.org/10.1093/idpl/ipz020**

SAFEnet. (2024). *Indonesia Digital Rights Report 2024: Trust, Transparency, and Accountability in the Age of Data*. SAFEnet.

Sugiyono. (2021). *Metode Penelitian Kuantitatif, Kualitatif, dan R&D*. Alfabeta.

Sudaryono, E. (2022). *Analisis hukum terhadap implementasi Undang-Undang Perlindungan Data Pribadi di Indonesia*. CV Mandar Maju.

Supomo, B. (2023). *Hukum Tata Kelola Data dan Perlindungan Privasi di Indonesia: Analisis Yuridis dan Komparatif*. Alumni Press.

World Bank. (2023). *Digital government readiness assessment: Indonesia country report*. World Bank Group.