

Personal Data Protection: The Effectiveness of Law Enforcement Mechanisms Against Privacy Violations in the Digital Economy Era

Reza Iswanto*

Batanghari University, Jambi, Indonesia

Abstract. *The digital economy has multiplied the collection, processing, and monetization of personal data, exposing individuals to escalating risks of privacy violation across e-commerce, fintech, and platform ecosystems. Although numerous jurisdictions have enacted comprehensive data protection statutes — Indonesia through Law No. 27 of 2022 on Personal Data Protection, the European Union through the General Data Protection Regulation, and India through the Digital Personal Data Protection Act 2023 — the effectiveness of their law enforcement mechanisms remains contested. This article examines the extent to which administrative, civil, and criminal enforcement instruments are capable of deterring and remedying privacy violations in the digital economy. Employing normative-juridical legal research grounded in statutory, conceptual, and comparative approaches, the study analyzes primary legal materials alongside recent scholarship addressing enforcement gaps, institutional capacity, and cross-border governance. The findings indicate that legislative enactment alone is insufficient; effectiveness depends on independent supervisory authorities, transparent sanction disclosure, adequate technical capacity, and harmonized cross-border cooperation. Indonesia's continuing absence of an operational Personal Data Protection Authority exemplifies the implementation gap common to emerging digital economies. The article concludes that a multi-track enforcement architecture combining administrative deterrence, civil remedies, and criminal sanctions, supported by institutional independence, is essential to closing the gap between legal text and behavioral compliance*

Keywords: *personal data protection; law enforcement; privacy violation; digital economy; regulatory effectiveness*

Received: 12 08, 2025 | **Revised:** 12 29, 2025 | **Accepted:** 01 17, 2026 | **Published Online:** 01 22, 2026

Correspondence:

Reza Iswanto

rezaiswanto17@gmail.com



1. Introduction

The digital economy has reconfigured personal data from an incidental by-product of transactions into a primary economic asset, generated at every point of contact between individuals and digital platforms, from marketplaces and ride-hailing applications to fintech and social media services.¹ This shift has been accompanied by an expansion of data-driven business models in which behavioral profiling, targeted advertising, and algorithmic decision-making rely on continuous, large-scale processing of consumers' personal information, often across distributed and cross-border infrastructures.² Empirical accounts of e-commerce data

¹Wang, C., Zhang, N., & Wang, Cong (2021). Managing privacy in the digital economy.

²Wang, Cui (2026). Data security and privacy protection in distributed digital economy.

breaches between 2018 and 2024 show that the pace of incidents has consistently outstripped the maturity of the institutions meant to prevent them, with third-party vendor compromises nearly doubling in a single year in some markets.³

In response, an increasing number of jurisdictions have enacted comprehensive personal data protection statutes over the past decade. A global review of privacy legislation shows convergence around core principles such as consent, purpose limitation, data minimization, and breach notification, even as enforcement architecture and institutional capacity diverge sharply between mature and emerging economies.⁴ Indonesia's Law No. 27 of 2022 on Personal Data Protection, which entered into full legal effect in October 2024, exemplifies this trend by adopting a GDPR-inspired structure of data-subject rights, controller obligations, and layered administrative, civil, and criminal sanctions. Comparable developments include India's Digital Personal Data Protection Act 2023, whose stakeholders across the legal, banking, and corporate sectors report substantial uncertainty about how the Act's Data Protection Board will translate statutory text into consistent enforcement practice.⁵ Similar patterns are visible in Vietnam's 2023 personal data decree governing e-commerce data controllers,⁶ the United Arab Emirates' civil data-protection framework,⁷ and India's fintech- and e-commerce-specific privacy regime.⁸

Despite this proliferation of statutes, a substantial body of scholarship documents a persistent gap between the enactment of data protection law and its practical enforcement. Cross-jurisdictional analysis of enforcement design finds that even well-resourced supervisory authorities struggle to translate broad statutory mandates into consistent investigation and sanctioning practice, producing what has been described as an enforcement gap between the promise of data-protection rights and their realization.⁹ World Bank research similarly finds that the cost of compliance with, and the cost of enforcing, data protection regulation are unevenly distributed, disadvantaging smaller economies and smaller firms that lack dedicated compliance infrastructure.¹⁰ In Indonesia, this pattern is visible in the continuing absence of the independent Personal Data Protection Authority mandated by the 2022 statute; without a

³Adu, I. (2026). Personal data protection in e-commerce platforms.

⁴Reis, O., Eneh, N. E., Ehimuan, B., Anyanwu, A., Olorunsogo, T., & Abrahams, T. O. (2024). Privacy law challenges in the digital age.

⁵Ahmed, S., & Nasir, M. (2026). Stakeholder perceptions of India's Digital Personal Data Protection Act of 2023.

⁶Nghia, L. T., & Tuan, N. M. (2026). Governance of consumers' personal data in e-commerce in Vietnam.

⁷Alhefeiti, A., Aldahmani, S. K. M. M., Alyammahi, A., Alzeyoudi, S. S. S. A., & Alraeesi, A. A. M. S. (2025). Civil protection of personal electronic data in the Emirati legislation.

⁸Singh, S., & Kumar, A. (2026). The right to privacy and the digital economy: an examination of India's data protection regime.

⁹Lancieri, F. (2021). Narrowing data protection's enforcement gap.

¹⁰Chander, A., Abraham, M., Chandy, S., Fang, Y., Park, D., & Yu, I. (2021). Achieving privacy: costs of compliance and enforcement of data protection regulation.

dedicated, adequately resourced supervisory body, existing enforcement provisions risk operating as a formal legal guarantee without corresponding institutional capacity to investigate, sanction, and remediate violations.¹¹ Strengthening the role of law enforcement in upholding privacy regulation is accordingly framed by recent Indonesian scholarship not merely as a technical compliance matter but as a question of national digital resilience.¹²

At the level of implementation, layered administrative, civil, and criminal sanctions have produced uneven results in practice. Studies of consumer data protection in Indonesia's digital economy find that administrative remedies are used more frequently than civil or criminal tracks, partly because dispute resolution outside the court system is procedurally simpler for aggrieved data subjects.¹³ Contractual misuse of consumer data in digital agreements remains difficult to redress under the Civil Code alone, reinforcing the need for the Personal Data Protection Law's more specific liability provisions to operate in tandem with civil procedure.¹⁴ Sector-specific evidence from online lending platforms illustrates how weak enforcement translates into tangible consumer harm, including unauthorized disclosure of borrowers' contact lists to third parties for debt-collection purposes.¹⁵ A civil-law enforcement pathway for personal data violations remains under-utilized in practice because data subjects rarely understand how to frame a claim for damages, and courts have limited precedent to draw on when quantifying non-material privacy harm.¹⁶

The cross-border and platform-mediated character of the digital economy compounds these domestic enforcement challenges. Because dominant technology platforms often function as de facto privacy regulators through their own terms of service and technical defaults, formal state enforcement authority may lag behind, or even depend upon, private platform governance choices.¹⁷ The tension between facilitating cross-border data flows for trade and safeguarding digital sovereignty produces a persistent legal dilemma for regulators seeking to enforce domestic data protection standards against foreign-based controllers.¹⁸ Comparative legal-support literature likewise emphasizes that harmonizing international compliance standards

¹¹Purnomo, H. (2026). Personal data protection in Indonesia's digital law enforcement system.

¹²Irfandi (2026). The role of law enforcement in upholding privacy regulations to strengthen national resilience in the digital era.

¹³Agustin, S. R., & Sodikin, S. (2026). Perlindungan hukum atas data pribadi konsumen dalam kegiatan ekonomi digital di Indonesia.

¹⁴Simanjuntak, F. A., Anjawai, N. B., Permatasari, R., & Rachmadhanto, D. A. S. (2026). Penyalahgunaan data pribadi konsumen dalam perjanjian digital berdasarkan KUHPERDATA dan Undang-Undang Perlindungan Data Pribadi.

¹⁵Magdalena, M. M. (2024). The online loans and protection of users' personal data: a normative judicial approach.

¹⁶Makkawaru, I. W., Nur, A. R., Djidar, H., & Mannuhung, S. (2025). Penegakan hukum perlindungan data pribadi melalui sarana hukum perdata.

¹⁷Hoboken, J., & Fathaigh, R. (2021). Smartphone platforms as privacy regulators.

¹⁸Kaya, M., & Shahid, H. (2025). Cross-border data flows and digital sovereignty: legal dilemmas in transnational governance.

with domestic cyber-law enforcement practice remains one of the most unresolved dimensions of cross-border personal data governance.¹⁹ The emergence of artificial intelligence-based processing adds a further layer of complexity: data protection authorities in the European Union already possess substantial experience relevant to AI-related enforcement, yet their institutional mandate for enforcing the forthcoming AI Act remains only partially defined, illustrating how regulatory design continually lags behind technological change.²⁰

Existing scholarship, however, tends to evaluate either the substantive adequacy of data protection statutes or country-specific enforcement case studies in isolation. A thirty-five-year systematic review of privacy law's legal evolution across the United States, the European Union, and other jurisdictions concludes that formal legal convergence has not been matched by convergence in enforcement effectiveness, leaving significant gaps in comparative understanding of what actually makes enforcement work.²¹ Economic-legal analysis further shows that privacy protection, data-sharing obligations, and market-opening objectives frequently pull enforcement priorities in different directions, a tension rarely addressed by studies that examine data protection law purely as a rights-protective instrument.²² Recent Indonesian scholarship similarly notes that cultural and societal attitudes toward privacy materially shape how vigorously data protection law is enforced in practice, a variable seldom integrated into formal legal-doctrinal analysis.²³ Global empirical mapping of breach incidents likewise demonstrates wide variation in the median scale of data leaked per sector and region, correlating loosely with the maturity of each jurisdiction's enforcement regime.

This article's novelty lies in three contributions that existing literature has not yet integrated. First, it synthesizes the effectiveness of three enforcement tracks administrative, civil, and criminal across jurisdictions positioned at markedly different levels of regulatory maturity, from the European Union to Indonesia, India, Vietnam, the United Arab Emirates, and the Russian Federation, rather than examining a single track or a single country in isolation. Second, it incorporates recent empirical evidence on the transparency of GDPR fine disclosure across national data protection authorities as a diagnostic benchmark for what “enforcement effectiveness” means beyond the mere existence of statutory sanctioning power.²⁴ Third,

¹⁹Khan, M. N. I. (2025). Cross-border data privacy and legal support: a systematic review of international compliance standards and cyber law practices.

²⁰Mazur, J., Novelli, C., & Choińska, Z. (2025). Should data protection authorities enforce the AI Act? Lessons from EU-wide enforcement data.

²¹Phang, K., & Kaabi, J. (2025). Privacy in flux: a 35-year systematic review of legal evolution, effectiveness, and global challenges.

²²Schäfer, H.-B. (2023). Current legal and economic problems of privacy protection, data sharing, and market-opening in the digital economy.

²³Mustafa, & Edy, S. S. (2026). Legal and cultural implications of personal data protection in the era of global digital society.

²⁴Baquero, P. M., Wang, A., & Restrepo Amariles, D. (2025). Unveiling transparency in data protection enforcement across the EU.

building on comparative lessons and on business-oriented analysis of personal data protection obligations in the digital economy,²⁵ it proposes a normative framework for strengthening Indonesia's institutional enforcement architecture, centered on the urgent establishment of an independent Personal Data Protection Authority (Lembaga Pelindungan Data Pribadi).

The remainder of this article proceeds as follows. Section 2 describes the normative-juridical research method employed. Section 3 presents the results and discussion, organized around administrative, civil, and criminal enforcement tracks, cross-border and institutional challenges, and a comparative table of six jurisdictions. Section 4 offers concluding remarks and policy recommendations.

2. Research Methods

This study employs normative-juridical (*yuridis normatif*) legal research, in which law is examined as a system of norms encompassing principles, rules, and doctrines contained in legislation, judicial decisions, and legal literature, rather than as a social fact to be measured through primary field data. The research draws on three complementary approaches: (1) the statute approach (statute approach), examining Indonesia's Law No. 27 of 2022 on Personal Data Protection alongside comparable instruments such as the European Union's General Data Protection Regulation and India's Digital Personal Data Protection Act 2023; (2) the conceptual approach (conceptual approach), analyzing doctrinal concepts of administrative, civil, and criminal enforcement and their theoretical relationship to legal effectiveness; and (3) the comparative approach (comparative approach), contrasting enforcement architecture across six jurisdictions to identify structural determinants of effectiveness.

The legal materials analyzed consist of primary sources (statutes, regulations, and official reports), secondary sources (peer-reviewed journal articles, books, and institutional studies), and tertiary sources (legal dictionaries and indexing databases) used to clarify terminology. Secondary literature was retrieved through academic search and citation-indexing platforms, including Google Scholar and Consensus, applying inclusion criteria that prioritized publications from the last five years (2021–2026) bearing an active, resolvable Digital Object Identifier (DOI), supplemented selectively by earlier foundational sources where doctrinally necessary. Data were analyzed using qualitative descriptive-analytical techniques: legal materials were systematized according to the three enforcement tracks under study, compared across jurisdictions, and interpreted in light of the general theory of legal effectiveness, which holds that a legal norm is effective only when it is accompanied by adequate institutional capacity, social awareness, and consistent implementation, not merely by its formal enactment.

²⁵Wijayanto, D. D., Indrayanti, K. W., & W, D. A. W. (2025). Personal data protection in digital business based on the Law on Personal Data Protection.

3. Result and Discussion

3.1 Administrative Enforcement

Administrative enforcement is the primary and most frequently invoked mechanism across the jurisdictions studied, typically comprising written warnings, temporary suspension of processing activities, mandated deletion or destruction of unlawfully processed data, and monetary fines calibrated as a percentage of annual revenue. Under Indonesia's Personal Data Protection Law, administrative fines may reach two percent of annual revenue or receipts, a ceiling markedly lower than the four percent of global annual turnover available under the General Data Protection Regulation. However, the mere existence of a fining power does not guarantee effective deterrence: empirical research across twenty-three of the European Union's twenty-seven data protection authorities finds substantial disparity in whether and how supervisory bodies publicly disclose the fines they impose, undermining the ability of researchers, policymakers, and the public to assess whether enforcement is in fact occurring at a level commensurate with the scale of violations.²⁶ If transparency deficits persist even within the European Union's comparatively mature enforcement ecosystem, the challenge is considerably greater in jurisdictions such as Indonesia, where the supervisory authority contemplated by the 2022 statute has yet to become operational, leaving the Ministry of Communication and Digital Affairs to exercise interim administrative enforcement without the institutional independence that specialized data protection authorities elsewhere are designed to provide.

Comparative research on Indonesia's digital law enforcement system confirms that the absence of an independent authority is the single most frequently cited structural weakness in the country's administrative enforcement track, producing delays in complaint handling and inconsistent sanctioning outcomes across sectors.²⁷ A related study similarly finds that legal problems in applying Indonesia's Personal Data Protection Law during the early years of its operation stem less from gaps in the statutory text itself than from the slow pace of issuing implementing regulations and establishing the institutions the law presupposes.²⁸ By contrast, India's Digital Personal Data Protection Act 2023 vests administrative enforcement in a dedicated Data Protection Board; stakeholder surveys nonetheless indicate that compliance preparedness varies markedly across the legal, banking, and corporate sectors, suggesting that

²⁶Baquero, P. M., Wang, A., & Restrepo Amariles, D. (2025). Unveiling transparency in data protection enforcement across the EU.

²⁷Purnomo, H. (2026). Personal data protection in Indonesia's digital law enforcement system.

²⁸Lutrianto, I., & Riswaldi, R. (2025). Legal problems of personal data protection in the digital era in Personal Data Protection Law in Indonesia.

formal institutional design alone does not eliminate uncertainty about how administrative enforcement will be exercised once the Board becomes fully active.²⁹

3.2 Civil Enforcement

Civil enforcement allows data subjects to seek compensation for material and non-material harm caused by unlawful processing, either through ordinary civil litigation or, where available, through dedicated data protection tribunals. Analysis of civil remedies under Indonesia's Personal Data Protection Law finds that this track remains structurally under-utilized because prospective claimants face high evidentiary burdens in proving both unlawful processing and quantifiable harm, and because litigation costs are frequently disproportionate to the compensation ultimately available.³⁰ Where consumer data is misused within digital agreements, reliance on the general tort provisions of the Civil Code alone has proven insufficient, reinforcing the argument that the Personal Data Protection Law's more specific data-subject rights must operate as a complementary, not a substitute, civil remedy.³¹

Consumer-protection-oriented analysis of Indonesia's digital economy similarly finds that civil remedies are most effective when paired with sector-specific consumer protection regulation, as in financial technology, where regulatory oversight bodies can order restitution alongside, or instead of, formal court proceedings.³² The Emirati experience offers a partial contrast: by codifying civil protection of personal electronic data directly within a dedicated legislative framework, rather than relying primarily on general tort principles, the United Arab Emirates provides data subjects with a comparatively clearer civil cause of action, though enforcement in practice still depends on judicial familiarity with data protection concepts that remain relatively novel.³³ Documented harm from unauthorized disclosure of borrower data on online lending platforms illustrates the practical stakes of an under-enforced civil track: without accessible and predictable compensation pathways, victims of privacy violations in high-volume digital lending markets are frequently left without effective redress.³⁴

²⁹Ahmed, S., & Nasir, M. (2026). Stakeholder perceptions of India's Digital Personal Data Protection Act of 2023.

³⁰Makkawaru, I. W., Nur, A. R., Djidar, H., & Mannuhung, S. (2025). Penegakan hukum perlindungan data pribadi melalui sarana hukum perdata.

³¹Simanjuntak, F. A., Anjawai, N. B., Permatasari, R., & Rachmadhanto, D. A. S. (2026). Penyalahgunaan data pribadi konsumen dalam perjanjian digital berdasarkan KUHPperdata dan Undang-Undang Perlindungan Data Pribadi.

³²Agustin, S. R., & Sodikin, S. (2026). Perlindungan hukum atas data pribadi konsumen dalam kegiatan ekonomi digital di Indonesia.

³³Alhefeiti, A., Aldahmani, S. K. M. M., Alyammahi, A., Alzeyoudi, S. S. S. A., & Alraeesi, A. A. M. S. (2025). Civil protection of personal electronic data in the Emirati legislation.

³⁴Magdalena, M. M. (2024). The online loans and protection of users' personal data: a normative judicial approach.

3.3 Criminal Enforcement

Criminal enforcement operates as the most severe, and correspondingly the most sparingly used, enforcement track, reserved for intentional or grossly negligent violations involving unlawful disclosure, sale, or falsification of personal data. Under Indonesia's Personal Data Protection Law, Articles 65 through 73 criminalize the unlawful obtaining, disclosure, and misuse of personal data, with penalties of imprisonment and substantial fines applicable to both natural persons and corporations. Case-level research within the jurisdiction of a regional police authority nonetheless documents recurring practical obstacles to criminal enforcement, including limited digital-forensic capacity, the technical complexity of tracing data flows across multiple intermediaries, and uncertainty among investigators about how to apply the relatively new statutory offenses.³⁵

A doctrinal study of legal responsibility for personal data violations under Indonesian law concludes that criminal sanctions, though normatively available, are applied inconsistently in practice, with administrative resolution frequently preferred by both regulators and defendants because it is faster and procedurally less demanding than criminal prosecution.³⁶ Comparative evidence from the Russian Federation reinforces this picture: criminal-law protection of personal data within a data-driven economy requires continual legislative updating to keep offense definitions aligned with evolving methods of data misuse, since static criminal provisions quickly become outpaced by new techniques of unlawful data exploitation.³⁷ Related Russian scholarship on the mechanism of criminal-law protection similarly emphasizes that personal data offenses often intersect with other cybercrime categories, such as fraud and identity theft, complicating both offense classification and sentencing.³⁸

3.4 Cross-Border, Platform, and Institutional Challenges

Because data controllers frequently operate across multiple jurisdictions through cloud infrastructure and multinational platforms, domestic enforcement authorities face structural limits on their investigative and sanctioning reach; dominant platforms often set de facto privacy standards through their own technical architecture before any regulator intervenes.³⁹ Reconciling the free flow of data necessary for cross-border trade with the exercise of domestic regulatory sovereignty remains a central and largely unresolved legal dilemma for transnational

³⁵Kasau, S., Husen, L., Thalib, H., & Arsyad, N. (2026). The essence of legal protection of personal data in electronic transactions within the jurisdiction of the South Sulawesi Regional Police.

³⁶Salsabila, S., & Wiraguna, S. A. (2025). Pertanggungjawaban hukum atas pelanggaran data pribadi dalam perspektif Undang-Undang Pelindungan Data Pribadi Indonesia.

³⁷Shutova, A., Begishev, I., & Volkova, A. (2026). Criminal law protection of personal data in a data economy.

³⁸Russkevich, E. (2023). Personal data in the mechanism of criminal law protection.

³⁹Hoboken, J., & Fathaigh, R. (2021). Smartphone platforms as privacy regulators.

data governance.⁴⁰ Comparative work situating cross-border trade governance alongside international legal frameworks similarly argues that principle-based, rather than purely rule-based, approaches to cross-border data flows may offer a more adaptable, though less predictable, basis for enforcement cooperation.⁴¹

A systematic review of cross-border data privacy and legal support arrangements finds that harmonizing international compliance standards with domestic cyber-law enforcement remains hampered by inconsistent mutual-recognition mechanisms between national authorities.⁴² Global visualization of data breach incidents across 2018–2019 further shows that the sectors and countries most affected by large-scale leaks are not necessarily those with the weakest formal legislation, but often those where enforcement institutions have not yet matured alongside the statute; extensive disclosure of sensitive records in some jurisdictions occurred notwithstanding the formal existence of applicable data protection law, underscoring that legislative text and enforcement capacity develop on different timelines.⁴³ The advent of artificial intelligence-driven processing adds an additional institutional design question: evidence on the activity level of European data protection authorities in AI-related enforcement suggests that, although these authorities possess relevant expertise, their formal mandate to serve as market surveillance authorities under the forthcoming AI Act remains only partially settled, illustrating how new technologies can outpace even comparatively mature enforcement institutions.⁴⁴

3.5 Comparative Overview

Table 1 synthesizes the enforcement architecture of six jurisdictions examined in this study, drawn from the statutory and comparative materials discussed above. The comparison highlights that enforcement maturity correlates more closely with the operational independence and resourcing of the supervisory authority than with the formal severity of statutory sanctions on paper.

⁴⁰Kaya, M., & Shahid, H. (2025). Cross-border data flows and digital sovereignty: legal dilemmas in transnational governance.

⁴¹Azam, M., Alwreikat, N., Alsyoud, B., Salam, A., Fandi, A. A. A., Abdul, R., & Pharaon, K. M. (2026). Contemporary trade governance and cross-border data flows: a comparative study of Sharī'ah principles and international legal frameworks.

⁴²Khan, M. N. I. (2025). Cross-border data privacy and legal support: a systematic review of international compliance standards and cyber law practices.

⁴³Pimenta Rodrigues, G. A., Marques Serrano, A. L., Lopes Espiñeira Lemos, A. N., Dias Canedo, E., Lúcio Lopes de Mendonça, F., de Oliveira Albuquerque, R., Sandoval Orozco, A. L., & García Villalba, L. J. (2024). Understanding data breach from a global perspective: incident visualization and data protection law review.

⁴⁴Mazur, J., Novelli, C., & Choińska, Z. (2025). Should data protection authorities enforce the AI Act? Lessons from EU-wide enforcement data.

Table 1. Comparative Overview of Personal Data Protection Enforcement Mechanisms in Selected Jurisdictions

Jurisdiction	Legal Basis	Supervisory Authority	Enforcement Tracks	Key Sanctions	Enforcement Maturity
Indonesia	Law No. 27/2022 on PDP	Interim: Ministry of Comm. & Digital Affairs; Authority not yet operational	Admin., civil, criminal	Fines up to 2% of revenue; up to 6 yrs prison (Arts. 65–73)	Emerging — in force since Oct. 2024; institution pending
European Union	Regulation (EU) 2016/679 (GDPR)	National DPAs in each Member State	Admin., civil, criminal (via national law)	Fines up to 4% of global turnover	Mature but uneven — fine-disclosure gaps across DPAs
India	Digital Personal Data Protection Act 2023	Data Protection Board of India	Admin. (primary); civil grievance redress	Financial penalties; grievance mechanism	Developing — uncertainty ahead of full enforcement
Vietnam	Decree 13/2023/ND-CP	Ministry of Public Security	Admin., criminal (via Penal Code)	Admin. fines; criminal liability for serious breaches	Emerging — capacity building underway
United Arab Emirates	Federal Decree-Law on PDP	UAE Data Office	Civil (codified), admin.	Civil compensation ; admin. penalties	Developing — limited judicial precedent
Russian Federation	Federal Law on Personal Data, as amended	Roskomnadzor	Admin., criminal	Admin. fines; imprisonment for aggravated offenses	Developing — offense definitions updated over time

As Table 1 illustrates, the depth of the enforcement toolkit on paper administrative, civil, and criminal tracks operating together — is broadly similar across the six jurisdictions. What differs substantially is the operational independence of the supervisory authority and the transparency with which enforcement outcomes are disclosed. This is consistent with findings that even within the European Union's comparatively resourced enforcement ecosystem, inconsistent public disclosure of fines by national authorities constrains the ability to verify whether statutory sanctioning power is being exercised proportionately to the scale of violations occurring.⁴⁵ The pattern suggests that legal effectiveness in this field should be assessed along at least four dimensions: (1) institutional independence of the supervisory authority; (2) technical and human-resource capacity for investigation, including digital forensics; (3) transparency and consistency of sanction disclosure; and (4) capacity for cross-border cooperation with foreign counterparts and platform operators. Business-oriented analysis of compliance obligations under Indonesia's Personal Data Protection Law similarly concludes that firms adjust their data-governance practices more in response to credible enforcement risk than to the abstract existence of statutory obligations, reinforcing the centrality of institutional capacity to effectiveness.⁴⁶

4. Conclusion

This article has examined the effectiveness of administrative, civil, and criminal law enforcement mechanisms against privacy violations in the digital economy, drawing on normative-juridical analysis of statutory materials and comparative scholarship across Indonesia, the European Union, India, Vietnam, the United Arab Emirates, and the Russian Federation. The analysis demonstrates that the proliferation of comprehensive data protection statutes over the past decade has not been matched by a corresponding proliferation of effective enforcement capacity. Administrative enforcement, though the most frequently used track, is constrained wherever supervisory authorities lack operational independence or fail to disclose sanctioning outcomes transparently. Civil enforcement remains structurally under-utilized due to evidentiary and cost barriers facing individual data subjects. Criminal enforcement, while normatively the most severe track, is applied inconsistently because of limited digital-forensic capacity and the continuing need to update offense definitions to match evolving methods of data misuse. Cross-border data flows and the growing role of dominant platforms and artificial intelligence systems further complicate the practical reach of domestic enforcement authorities.

For Indonesia specifically, the findings underscore that the establishment of an independent, adequately resourced Personal Data Protection Authority should be treated as an urgent institutional priority rather than a procedural formality, since the absence of such an authority is the single most consistently identified obstacle to effective enforcement in the

⁴⁵Baquero, P. M., Wang, A., & Restrepo Amariles, D. (2025). Unveiling transparency in data protection enforcement across the EU.

⁴⁶Wijayanto, D. D., Indrayanti, K. W., & W, D. A. W. (2025). Personal data protection in digital business based on the Law on Personal Data Protection.

literature reviewed. Complementary measures should include clearer procedural guidance to lower evidentiary and cost barriers for civil claims, investment in digital-forensic capacity to support criminal prosecutions, transparent public reporting of administrative sanctions to enable external accountability, and active participation in regional and international cooperation mechanisms to address cross-border violations. More broadly, this study suggests that the effectiveness of personal data protection law should be evaluated not by the existence or severity of statutory sanctions alone, but by the institutional independence, technical capacity, transparency, and cross-border cooperation that give those sanctions practical force. Future research employing empirical and socio-legal methods would usefully test the framework proposed here against enforcement outcomes as Indonesia's Personal Data Protection Authority, once established, begins to operate

References

- Adu, I. (2026). Personal data protection in e-commerce platforms: Legal challenges, regulatory frameworks, and the path toward digital consumer trust. *Privet Social Sciences Journal*, 6(5), 118–128. <https://doi.org/10.55942/pssj.v6i5.1815>
- Agustin, S. R., & Sodikin, S. (2026). Perlindungan hukum atas data pribadi konsumen dalam kegiatan ekonomi digital di Indonesia. *AHKAM*, 5(3). <https://doi.org/10.58578/ahkam.v5i3.10637>
- Ahmed, S., & Nasir, M. (2026). Stakeholder perceptions of India's Digital Personal Data Protection Act of 2023: An empirical study across legal, banking, and corporate sectors. *Frontiers in Sociology*, 11. <https://doi.org/10.3389/fsoc.2026.1753383>
- Alhefeiti, A., Aldahmani, S. K. M. M., Alyammahi, A., Alzeyoudi, S. S. S. A., & Alraeesi, A. A. M. S. (2025). Civil protection of personal electronic data in the Emirati legislation. *Research Journal in Advanced Humanities*. <https://doi.org/10.58256/lakswg81>
- Azam, M., Alwreikat, N., Alsyouf, B., Salam, A., Fandi, A. A. A., Abdul, R., & Pharaon, K. M. (2026). Contemporary trade governance and cross-border data flows: A comparative study of Shari'ah principles and international legal frameworks. *MILRev: Metro Islamic Law Review*, 5(1). <https://doi.org/10.32332/milrev.v5i1.13387>
- Baquero, P. M., Wang, A., & Restrepo Amariles, D. (2025). Unveiling transparency in data protection enforcement across the EU: Assessing the level and quality of disclosure of GDPR fines by data protection authorities. *European Law Journal*. <https://doi.org/10.1111/eulj.70008>
- Chander, A., Abraham, M., Chandy, S., Fang, Y., Park, D., & Yu, I. (2021). Achieving privacy: Costs of compliance and enforcement of data protection regulation (Policy Research Working Paper). World Bank. <https://doi.org/10.1596/1813-9450-9594>
- Hoboken, J., & Fathaigh, R. (2021). Smartphone platforms as privacy regulators. *Computer Law & Security Review*, 41. <https://doi.org/10.1016/j.clsr.2021.105557>

- Irfandi. (2026). The role of law enforcement in upholding privacy regulations to strengthen national resilience in the digital era. *Multidisciplinary Indonesian Center Journal (MICJO)*, 3(1). <https://doi.org/10.62567/micjo.v3i1.1790>
- Kasau, S., Husen, L., Thalib, H., & Arsyad, N. (2026). The essence of legal protection of personal data in electronic transactions within the jurisdiction of the South Sulawesi Regional Police. *Veredas do Direito*, 23. <https://doi.org/10.18623/rvd.v23.6690>
- Kaya, M., & Shahid, H. (2025). Cross-border data flows and digital sovereignty: Legal dilemmas in transnational governance. *Interdisciplinary Studies in Society, Law, and Politics*, 4(2). <https://doi.org/10.61838/kman.isslp.4.2.20>
- Khan, M. N. I. (2025). Cross-border data privacy and legal support: A systematic review of international compliance standards and cyber law practices. *American Journal of Scholarly Research and Innovation*. <https://doi.org/10.63125/a4gbeb22>
- Kurdi, & Cahyono, J. (2024). Perlindungan data pribadi di era digital berdasarkan Undang-Undang Nomor 27 Tahun 2022. *JUNCTO: Jurnal Ilmiah Hukum*, 6(2). <https://doi.org/10.31289/juncto.v6i2.5443>
- Lancieri, F. (2021). Narrowing data protection's enforcement gap. *SSRN Electronic Journal*. <https://doi.org/10.2139/ssrn.3806880>
- Lutrianto, I., & Riswaldi, R. (2025). Legal problems of personal data protection in the digital era in Personal Data Protection Law in Indonesia. *Greenation International Journal of Law and Social Sciences*, 3(2). <https://doi.org/10.38035/gijlss.v3i2.429>
- Magdalena, M. M. (2024). The online loans and protection of users' personal data: A normative judicial approach. *Pena Justisia: Media Komunikasi dan Kajian Hukum*, 23(1). <https://doi.org/10.31941/pj.v23i1.5375>
- Makkawaru, I. W., Nur, A. R., Djidar, H., & Mannuhung, S. (2025). Penegakan hukum perlindungan data pribadi melalui sarana hukum perdata. *Journal of Innovation Research and Knowledge*, 4(9), 6473–6488. <https://doi.org/10.53625/jirk.v4i9.9663>
- Mazur, J., Novelli, C., & Chońska, Z. (2025). Should data protection authorities enforce the AI Act? Lessons from EU-wide enforcement data. *International Data Privacy Law*. <https://doi.org/10.1093/idpl/ipaf033>
- Mustafa, & Edy, S. S. (2026). Legal and cultural implications of personal data protection in the era of global digital society. *Jurnal Hukum Caraka Justitia*, 6(1). <https://doi.org/10.30588/jhcj.v6i1.2496>
- Nghia, L. T., & Tuan, N. M. (2026). Governance of consumers' personal data in e-commerce in Vietnam. *Veredas do Direito*, 23. <https://doi.org/10.18623/rvd.v23.5186>
- Phang, K., & Kaabi, J. (2025). Privacy in flux: A 35-year systematic review of legal evolution, effectiveness, and global challenges (U.S./E.U. focus with international comparisons). *Journal of Cybersecurity and Privacy*, 5(4), 103. <https://doi.org/10.3390/jcp5040103>
- Pimenta Rodrigues, G. A., Marques Serrano, A. L., Lopes Espiñeira Lemos, A. N., Dias Canedo, E., Lúcio Lopes de Mendonça, F., de Oliveira Albuquerque, R., Sandoval

- Orozco, A. L., & García Villalba, L. J. (2024). Understanding data breach from a global perspective: Incident visualization and data protection law review. *Data*, 9(2), 27. <https://doi.org/10.3390/data9020027>
- Purnomo, H. (2026). Personal data protection in Indonesia's digital law enforcement system. *AKSELERASI: Jurnal Ilmiah Nasional*, 8(1). <https://doi.org/10.54783/jin.v8i1.1762>
- Reis, O., Eneh, N. E., Ehimuan, B., Anyanwu, A., Olorunsogo, T., & Abrahams, T. O. (2024). Privacy law challenges in the digital age: A global review of legislation and enforcement. *International Journal of Applied Research in Social Sciences*, 6(1). <https://doi.org/10.51594/ijarss.v6i1.733>
- Russkevich, E. (2023). Personal data in the mechanism of criminal law protection. *Proceedings of Southwest State University. Series: History and Law*, 13(5), 75–86. <https://doi.org/10.21869/2223-1501-2023-13-5-75-86>
- Salsabila, S., & Wiraguna, S. A. (2025). Pertanggungjawaban hukum atas pelanggaran data pribadi dalam perspektif Undang-Undang Pelindungan Data Pribadi Indonesia. *Konsensus: Jurnal Ilmu Pertahanan, Hukum dan Ilmu Komunikasi*, 2(2). <https://doi.org/10.62383/konsensus.v2i2.736>
- Schäfer, H.-B. (2023). Current legal and economic problems of privacy protection, data sharing, and market-opening in the digital economy. *The Antitrust Bulletin*, 68(4), 641–656. <https://doi.org/10.1177/0003603x231200938>
- Shutova, A., Begishev, I., & Volkova, A. (2026). Criminal law protection of personal data in a data economy. *Law Enforcement Review*, 10(2), 127–136. [https://doi.org/10.52468/2542-1514.2026.10\(2\).127-136](https://doi.org/10.52468/2542-1514.2026.10(2).127-136)
- Simanjuntak, F. A., Anjawai, N. B., Permatasari, R., & Rachmadhanto, D. A. S. (2026). Penyalahgunaan data pribadi konsumen dalam perjanjian digital berdasarkan KUHPdata dan Undang-Undang Perlindungan Data Pribadi. *Jurnal Alwatzikhoebillah: Kajian Islam, Pendidikan, Ekonomi, Humaniora*, 12(1). <https://doi.org/10.37567/alwatzikhoebillah.v12i1.5135>
- Singh, S., & Kumar, A. (2026). The right to privacy and the digital economy: An examination of the impact of India's data protection regime on e-commerce and fintech. *EPRA International Journal of Research & Development (IJRD)*. <https://doi.org/10.36713/epra25992>
- Wang, C., Zhang, N., & Wang, Cong. (2021). Managing privacy in the digital economy. *Fundamental Research*. <https://doi.org/10.1016/j.fmre.2021.08.009>
- Wang, Cui. (2026). Data security and privacy protection in distributed digital economy: Economic impacts and governance mechanisms. *ICST Transactions on Scalable Information Systems*. <https://doi.org/10.4108/eetsis.12557>
- Wijayanto, D. D., Indrayanti, K. W., & W, D. A. W. (2025). Personal data protection in digital business based on the Law on Personal Data Protection. *International Journal of Research in Social Science and Humanities*, 8. <https://doi.org/10.47505/ijrss.2025.8.2>