

Personal Data Protection in the Artificial Intelligence Era: Evaluating the Implementation of Indonesia's Law No. 27 of 2022

Siti Aisah Ajahra¹, Hilman Nur²

^{1,2} Universitas Suryakencana, Indonesia

correspondence: raraazzahra62198@gmail.com

Article Information

Article History:

Received Jun 01th, 2026

Revised Sept 21th, 2026

Accepted Sept 26th, 2026

Keyword:

personal data protection; artificial intelligence; privacy; cyber law; automated decision-making; Indonesia

ABSTRACT

This study evaluated the implementation of Indonesia's Law No. 27 of 2022 on Personal Data Protection in the context of rapid digitalization and artificial intelligence. A socio-legal empirical design was employed by combining statutory and conceptual analysis with questionnaire data from 49 respondents and qualitative stakeholder material. The findings showed that the Law established a substantially stronger rights-based framework, including rights of access, correction, erasure, withdrawal of consent, data portability, and objection to solely automated decisions. Nevertheless, implementation remained uneven. Respondents demonstrated moderate awareness of data-subject rights, while perceived protection, government socialization, complaint accessibility, deterrent effect, and overall effectiveness remained limited. Artificial intelligence intensified these implementation challenges because profiling, biometric processing, model training, and automated decision-making increased the scale and opacity of personal-data processing. The study concluded that effective protection required stronger supervision, clearer implementing rules, enforceable accountability, privacy-by-design practices, improved cyber security, and sustained public digital-literacy programs.



© 2025 Para Penulis. Diterbitkan oleh Riset Anak Bangsa. Ini adalah artikel akses terbuka di bawah lisensi CC BY (<https://creativecommons.org/licenses/by/4.0/>)

INTRODUCTION

Digital transformation has made the processing of personal data a routine condition of social, economic, educational, financial, health, and governmental activity. Individuals continuously disclose identifiers, location information, transaction histories, communication records, biometric attributes, behavioral traces, and other information to digital platforms. The resulting data ecosystem has created substantial social and economic value, yet it has also increased the risks of unlawful collection, identity theft, profiling, discriminatory treatment, data leakage, and cyber-enabled fraud. In this environment, personal data protection is no longer a peripheral aspect of information-technology governance; it is an essential component of privacy, human dignity, legal certainty, and trust in digital services. Manurung (2023) accordingly locates personal data protection within the constitutional right to privacy, while Kurniawan et al. (2024) emphasize that a comprehensive statutory framework must be accompanied by institutional capacity and effective enforcement.

Indonesia responded to the fragmentation of earlier sectoral rules by enacting Law No. 27 of 2022 on Personal Data Protection (the PDP Law). The statute applies to personal-data processing carried out within Indonesia and, under specified conditions, to processing outside Indonesian territory that produces legal consequences in Indonesia or for Indonesian citizens. It categorizes general and specific personal data, establishes rights of data subjects, regulates lawful bases and principles for processing, assigns obligations to controllers and processors, governs transfers, provides administrative and criminal sanctions, and establishes a legal basis for a supervisory institution. The law therefore represents a structural shift from dispersed sectoral protection toward an integrated legal framework (Republic of Indonesia, 2022; Simbolon & Juwono, 2022).

The transition is particularly important because the risks addressed by the PDP Law are evolving alongside artificial intelligence (AI). Contemporary AI systems are data-intensive. Machine-learning models may rely on large datasets for training, validation, personalization, prediction, classification, and automated decision-making. Personal data may be processed directly, inferred from apparently non-sensitive variables, or incorporated into probabilistic profiles. AI can also increase the persistence of data by embedding statistical information in model parameters and can make processing

less transparent because outcomes may result from complex computational relationships that are difficult for ordinary users to understand. Meurisch and Mühlhäuser (2021) show that data protection in AI services cannot be secured through a single technical measure; it requires coordinated management, system-level, and AI-level safeguards. Similarly, van Bakkum and Zuiderveen Borgesius (2023) demonstrate that AI creates difficult tensions between sensitive-data restrictions and the need to detect or mitigate algorithmic discrimination.

The PDP Law contains provisions that are directly relevant to AI governance. In addition to rights of access, correction, erasure, withdrawal of consent, and portability, Article 10 recognizes the right of a data subject to object to a decision based solely on automated processing, including profiling, where the decision produces legal consequences or a significant effect. This provision is conceptually important because it recognizes that harm may arise not only from disclosure or theft of data, but also from how data are analyzed and used to make consequential decisions. Comparable debates under the European Union's General Data Protection Regulation (GDPR) indicate that meaningful contestability requires more than a formal notice. It depends on understandable information, a genuine possibility of review, procedural safeguards, and institutional mechanisms capable of examining automated decision-making (Bayamlioğlu, 2022; European Parliament & Council, 2016).

Despite this normative progress, the central question is whether the PDP Law has translated into effective protection in practice. A legal rule may be comprehensive on paper yet remain ineffective when institutions lack capacity, organizations do not redesign their data-governance practices, citizens do not understand their rights, complaint mechanisms are difficult to access, or sanctions are not predictably enforced. Recent Indonesian scholarship has repeatedly identified this implementation gap. Rinjani and Firmansyah (2025) point to weak enforcement, institutional overlap, and limited accountability. Widiatedja and Mishra (2023) argue that effective data protection requires an adequately independent supervisory authority with clear powers and resources. Neta et al. (2022) similarly emphasize the urgency of an independent supervisory structure, while Kholis (2025) illustrates how cyber-security incidents in the banking sector expose the practical interaction between regulatory duties and technological readiness.

Comparative studies also demonstrate that the effectiveness of a data-protection regime depends on the relationship between legal principles and operational compliance. Simbolon and Juwono (2022) find substantial convergence between the Indonesian PDP Law and the GDPR regarding data-subject rights, but identify differences in regulatory detail and sanctioning mechanisms. Soemitro et al. (2023) show that Indonesia has adopted significant penal provisions, yet deterrence depends on how sanctions are applied rather than merely on their formal severity. Tikkinen-Piri et al. (2018), examining GDPR implementation, conclude that compliance requires substantial organizational changes, training, resources, risk management, and technological adaptation. These insights are particularly relevant to Indonesian small and medium-sized organizations, public bodies, and digital businesses that may have different levels of compliance maturity.

Previous studies have generally focused on normative comparison, institutional design, criminal sanctions, sector-specific security, or emerging technologies. Mayasari (2023), for example, examines personal-data risks in metaverse environments, while studies of data portability and digital services highlight the growing importance of data-subject control in increasingly interconnected ecosystems (Wiwoho et al., 2024). However, fewer studies combine the legal structure of the PDP Law with empirical perceptions of implementation and then relate those perceptions specifically to AI-driven processing. This produces a research gap: the Indonesian framework needs to be evaluated simultaneously as a legal architecture, an implementation system, and a foundation for protecting individuals against the distinctive risks of automated and data-intensive technologies.

This study therefore aimed to evaluate the implementation of Law No. 27 of 2022 by integrating socio-legal empirical findings with statutory and conceptual analysis. It addressed three questions. First, to what extent does the PDP Law provide an adequate legal framework for personal-data protection, including in AI-enabled environments? Second, how do respondents perceive awareness, protection, socialization, complaint accessibility, deterrence, and overall effectiveness after the law's enactment? Third, what legal, institutional, technological, and social measures are required to strengthen implementation? The contribution of the study lies in connecting the formal rights and obligations contained in the law with observed implementation perceptions and with the additional governance

demands created by AI, especially profiling, biometrics, automated decision-making, and large-scale data processing.

RESEARCH METHOD

This research used a socio-legal empirical design supported by statutory and conceptual approaches. The empirical dimension was retained because the author-provided study collected primary information from users and stakeholders regarding their understanding and perceptions of personal-data protection. The legal dimension was necessary to evaluate those perceptions against the rights, obligations, supervisory mechanisms, and sanctions established by Law No. 27 of 2022. This combination enabled the research to move beyond a purely doctrinal description of the statute and to examine the distance between legal norms and perceived implementation.

The statutory approach focused primarily on Law No. 27 of 2022 on Personal Data Protection, with particular attention to the categories of personal data, rights of data subjects, principles and lawful bases of processing, controller and processor obligations, automated decision-making, security, breach response, supervision, dispute settlement, and sanctions. The analysis also used the GDPR as a comparative reference for issues of accountability, automated decision-making, and organizational compliance. Comparative material was not employed to claim that the Indonesian regime must reproduce European law, but to identify governance mechanisms that clarify how broad data-protection principles may be operationalized in practice (Simbolon & Juwono, 2022; Tikkinen-Piri et al., 2018).

The empirical material consisted of questionnaire data from 49 valid respondents and qualitative stakeholder material collected through the procedures described in the original study, including semi-structured interviews and documentary observation. Purposive sampling was used to reach persons considered relevant to the implementation of personal-data protection, including users of digital services and stakeholders familiar with legal, organizational, or information-technology aspects of data processing. Because the available author dataset did not provide a separate numerical breakdown for each stakeholder category, the analysis did not infer demographic composition that was not documented in the source material.

The questionnaire examined respondents' understanding of data-subject rights, perceptions of increased protection after the PDP Law, perceptions of government socialization, accessibility of complaint mechanisms, perceived deterrent effect of statutory sanctions, and overall effectiveness. For data-integrity purposes, the quantitative analysis reported only questionnaire items whose response counts and percentages were internally consistent in the author-provided tabulation. Items that required reconfirmation against the raw questionnaire records were not used as numerical evidence. This revision strategy avoided correcting uncertain values by assumption and ensured that every percentage interpreted in the results could be reproduced from the reported respondent total.

Quantitative responses were analyzed descriptively through frequencies and percentages. The empirical findings were then interpreted through qualitative legal analysis. This analysis proceeded in four stages: identifying the relevant statutory rule; describing the empirical perception associated with the rule; comparing the finding with recent scholarly research; and evaluating implications for implementation in AI-intensive digital environments. The analytical standard for legal effectiveness was therefore multidimensional. A provision was not treated as effective merely because it existed in the statute; effectiveness was assessed in relation to public awareness, organizational readiness, accessibility of enforcement mechanisms, institutional supervision, technological safeguards, and the ability of data subjects to exercise rights in practice.

The study's scope should be understood as evaluative rather than nationally representative. The sample size does not permit generalization to the entire Indonesian population, and the available dataset does not support causal inference. The value of the empirical component lies instead in identifying implementation signals that can be examined against the legal framework and prior research. This limitation is especially important when discussing AI, because the questionnaire was designed around general personal-data protection rather than specific experiences with algorithmic systems. Accordingly, the AI analysis is grounded in the statute and relevant literature and is used to interpret the future-facing implications of the empirical implementation gaps, not to claim that respondents directly evaluated particular AI models.

RESULTS AND DISCUSSION

Legal Architecture of the PDP Law and its Relevance to Artificial Intelligence

Law No. 27 of 2022 provides a substantially more coherent legal foundation for personal-data protection than the earlier fragmented sectoral approach. Its definition of personal data covers information relating to an identified or identifiable individual, whether processed electronically or non-electronically. The distinction between general and specific personal data is significant for AI because data and information concerning health, biometrics, genetics, children, criminal records, and personal finances may be particularly attractive for prediction and classification while simultaneously producing severe harms when misused. AI systems that process facial templates, health indicators, credit characteristics, behavioral patterns, or children's online activity therefore engage the statute not only at the point of collection but throughout the processing lifecycle.

The statute's data-subject rights establish a rights-based architecture that can constrain data-intensive technologies. Rights to information, correction, access, erasure, withdrawal of consent, processing limitation, compensation, and portability collectively enable individuals to challenge the assumption that data controllers have unlimited discretion once information has been collected. Manurung (2023) correctly connects these protections to privacy as a constitutional interest rather than a merely contractual preference. Data portability is also increasingly important because contemporary digital services operate through interconnected platforms and application programming interfaces. Wiwoho et al. (2024) show, in the context of open banking, that portability can support both individual control and competition when technical interoperability and legal safeguards are appropriately balanced.

Article 10 is especially relevant to the AI era because it recognizes a right to object to decisions based solely on automated processing, including profiling, where legal or significant effects arise. This provision creates a bridge between data-protection law and algorithmic governance. A credit score, employment screening result, insurance risk classification, education-admission filter, fraud-detection flag, or other automated assessment can affect an individual without exposing the underlying personal data to the public. The legal harm may therefore arise from the decision produced from data rather than from the disclosure of data itself. Bayamlıoğlu (2022) demonstrates that contesting automated decisions requires a procedural perspective: the individual must be able to understand that automation has occurred, challenge relevant inputs or inferences, and obtain meaningful review. Indonesia's Article 10 provides an important normative starting point, but its effectiveness depends on detailed procedures, organizational documentation, human review, and an accessible supervisory process.

AI also complicates traditional concepts of consent and purpose limitation. Data collected for one service may later become attractive for model training, fraud analytics, behavioral advertising, or product development. Yet the legal basis for the original processing does not automatically legitimize every new analytical purpose. Data minimization is similarly difficult when model developers assume that more data will produce better predictions. Tikkinen-Piri et al. (2018) show that effective data-protection compliance requires organizations to translate legal principles into operational data-management rules, while Meurisch and Mühlhäuser (2021) emphasize the need for privacy controls at organizational, system, and model levels. In the Indonesian context, this means that controllers cannot treat cyber security alone as full compliance. Security reduces unauthorized access, but lawful purpose, transparency, accuracy, fairness, retention limits, and data-subject rights remain separate obligations.

The problem becomes more complex where AI derives sensitive characteristics from ordinary data. Even if an organization does not explicitly collect health status, political preference, or other sensitive information, a model may infer such attributes from browsing behavior, purchasing patterns, location traces, language, or social relationships. Van Bekkum and Zuiderveen Borgesius (2023) show that the relationship between sensitive data and anti-discrimination safeguards is legally difficult because detecting algorithmic bias may itself require protected attributes. The PDP Law's implementation framework should therefore account for inferred data and high-risk profiling, not only databases containing explicitly labeled sensitive fields. This is one reason why impact assessments, documentation, auditability, and human oversight should be treated as practical expressions of statutory accountability in AI-intensive processing.

The law's sanctioning framework is comparatively strong on paper. It combines administrative measures with criminal provisions for unlawful collection, disclosure, use, and falsification of personal data. Corporate liability and additional penalties can also apply. Soemitro et al. (2023) note that Indonesia adopts significant criminal sanctions in comparison with Singapore. However, the existence of severe penalties does not by itself establish deterrence. Deterrence depends on the probability of

detection, clarity of responsibility, quality of investigation, institutional coordination, and consistency of enforcement. These practical conditions become more important where AI processing is distributed across data controllers, cloud providers, software vendors, model developers, and third-party data sources. Accountability must be mapped across that chain so that technological complexity does not become a mechanism for avoiding legal responsibility.

Empirical Perceptions of Implementation Effectiveness

The questionnaire results provide a useful indication of how the law's implementation is perceived at the user level. Table 1 presents the six items for which the author-provided counts were internally consistent at $n = 49$. The data show a clear distinction between awareness of rights and confidence in enforcement. Nearly two thirds of respondents stated that they understood their rights as personal-data owners, but substantially fewer felt that their data had become more protected after the law was enacted. Perceptions of government socialization, complaint accessibility, deterrence, and overall effectiveness were also mixed or negative. These findings suggest that formal legal awareness has developed faster than institutional trust and practical experience of protection.

Table 1 Respondents' Perceptions of PDP Law Implementation ($n = 49$)

No.	Question / indicator	Yes	No	Unsure / other
1	Understanding of rights as a personal-data subject	32 (65.3%)	7 (14.3%)	10 (20.4%)
2	Feeling more protected after enactment of the PDP Law	19 (38.8%)	14 (28.6%)	16 (32.7%)
3	Government socialization considered sufficient	16 (32.7%)	16 (32.7%)	17 (34.7%)
4	Complaint mechanism considered easy to access	14 (28.6%)	18 (36.7%)	17 (34.7%)
5	Sanctions considered sufficiently deterrent	17 (34.7%)	5 (10.2%)	27 (55.1%)
6	Overall implementation considered effective	15 (30.6%)	16 (32.7%)	18 (36.7%)

Note. Only items with internally consistent totals in the author-provided tabulation are reported quantitatively.

The strongest positive finding concerned awareness of rights: 65.3% of respondents reported understanding their rights, while 14.3% reported that they did not and 20.4% were uncertain. This level of awareness is encouraging because rights are meaningful only when data subjects know that they can request information, access data, seek correction, withdraw consent, request deletion under applicable conditions, or pursue remedies. Nevertheless, approximately one third of respondents did not clearly understand those rights. The result is consistent with the continuing need for public education identified by Rinjani and Firmansyah (2025). Awareness should therefore be treated as an implementation obligation shared across government, educational institutions, civil society, and data controllers rather than as a one-time socialization campaign.

Perceived improvement in protection was markedly weaker. Only 38.8% of respondents felt more protected after the PDP Law, compared with 28.6% who did not and 32.7% who were uncertain. This gap between legal awareness and felt protection is analytically important. A citizen may know that a law exists but still doubt whether an organization will respond to a request, whether a complaint will be processed, whether a breach will be investigated, or whether compensation and sanctions will be realistic. Kurniawan et al. (2024) similarly conclude that the Indonesian framework is legally substantial but requires institutional strengthening, while Kholis (2025) shows that operational cyber-security failures can undermine confidence even where formal legal duties are clear.

Government socialization was also perceived as insufficient or uncertain. The responses were almost evenly distributed: 32.7% considered socialization sufficient, 32.7% considered it insufficient, and 34.7% were unsure. This result indicates that the communication of the law has not yet produced consistent public understanding. Socialization in the AI era must extend beyond warnings not to share passwords or one-time passwords. Citizens need understandable information about profiling, biometric processing, automated decisions, data portability, consent withdrawal, and complaint rights. Without this broader literacy, individuals may consent to complex processing without appreciating how data can be combined, inferred, or reused by algorithmic systems.

The accessibility of complaint mechanisms produced a more clearly negative signal. Only 28.6% regarded complaint mechanisms as easy to access, whereas 36.7% did not and 34.7% were unsure. In practical terms, a right that cannot be exercised through a clear and responsive procedure is weakened. Effective implementation therefore requires a visible complaint pathway, defined response

periods, case-tracking, rules for evidence preservation, and coordination between the data-protection authority and sectoral regulators or law-enforcement bodies. Widiatedja and Mishra (2023) argue that supervisory independence and institutional competence are central to meaningful data protection, while Neta et al. (2022) emphasize that the authority must be designed to avoid fragmented and ineffective oversight.

The survey also reveals uncertainty about deterrence. Although 34.7% considered sanctions sufficiently deterrent, 55.1% were unsure. Only 10.2% expressly considered them non-deterrent. The high level of uncertainty is itself significant because deterrence depends partly on the visibility and predictability of enforcement. Severe statutory penalties can have limited behavioral effect if organizations and citizens rarely observe how violations are investigated, how administrative sanctions are calculated, how corporate responsibility is assigned, or how victims obtain redress. This finding supports Soemitro et al.'s (2023) argument that comparative differences in sanction severity do not answer the more difficult implementation question of how sanctions are applied.

Finally, only 30.6% of respondents considered overall implementation effective, while 32.7% considered it ineffective and 36.7% were unsure. The combined majority of negative and uncertain responses demonstrates that the law's legitimacy cannot be measured solely by enactment. For users, implementation is experienced through privacy notices, consent interfaces, security incidents, complaint handling, organizational responses, and visible enforcement. The result is therefore consistent with an implementation-stage regulatory regime: the legal framework has created rights and duties, but citizens have not uniformly experienced those rights and duties as reliable protection.

Institutional, Technological, and Organizational Barriers

The empirical findings are best understood as the product of interacting institutional, technological, organizational, and social barriers. Institutionally, the effectiveness of the PDP Law depends on a supervisory architecture capable of issuing guidance, receiving complaints, conducting investigations, coordinating across sectors, evaluating cross-border transfers, and imposing administrative sanctions. The statute itself assigns extensive powers to the supervisory institution. However, the practical value of those powers depends on independence, staffing, technical expertise, investigative capacity, procedural transparency, and coordination with existing regulators. Widiatedja and Mishra (2023) argue that independence is particularly important because data-protection disputes may involve both private corporations and public bodies. Oversight that is perceived as institutionally weak can reduce both compliance incentives and public confidence.

Organizational readiness is another major barrier. Compliance requires controllers to know what personal data they hold, why the data were collected, the legal basis for each processing activity, where data are stored, who receives them, how long they are retained, and what technical and organizational safeguards apply. These tasks require data inventories, access-control rules, vendor management, retention schedules, incident-response procedures, staff training, and documented decision-making. Tikkinen-Piri et al. (2018) emphasize that data-protection reform has strategic, organizational, and technical implications and cannot be implemented by revising a privacy policy alone. This insight is directly relevant to Indonesian organizations that may formally publish privacy notices while lacking mature internal governance.

Cyber security is closely related to, but distinct from, legal compliance. Encryption, multi-factor authentication, access controls, network monitoring, secure development, backups, vulnerability management, and incident response reduce the likelihood and impact of unauthorized access. Kholis (2025) shows that sectoral implementation problems can become visible through ransomware and other cyber incidents. Yet the PDP Law requires a broader concept of accountability. A perfectly secure system may still violate data-protection principles if it collects excessive data, lacks a lawful basis, retains information indefinitely, or uses personal data for incompatible purposes. Conversely, an organization may have a valid legal basis but still fail if its security practices are inadequate. Effective implementation requires both dimensions.

AI introduces additional organizational complexity because responsibility may be distributed between data controllers and technology suppliers. An organization can purchase an AI service without fully understanding the training data, model behavior, logging architecture, or sub-processors involved. The organization may nevertheless remain responsible for deciding why and how personal data are used. Vendor contracts therefore need to define processing instructions, confidentiality, security

requirements, breach notification, audit rights, deletion, cross-border processing, and assistance with data-subject requests. Where AI models are used for consequential decisions, documentation should also record model purpose, data sources, risk assessment, performance limitations, human-review procedures, and mechanisms for contesting outcomes.

A further barrier is the tendency to reduce privacy governance to consent. Consent is important but cannot serve as a universal justification for complex processing. In digital environments, users often confront long privacy notices, bundled choices, or take-it-or-leave-it interfaces. AI makes the problem more difficult because future uses or model inferences may not be easily foreseeable at the moment of collection. The PDP Law already recognizes multiple lawful bases for processing; implementation should therefore require controllers to select and document the appropriate legal basis rather than routinely seeking broad consent. Where consent is used, it should be specific, informed, demonstrable, and withdrawable without making the withdrawal procedure disproportionately difficult.

Small and medium-sized enterprises face particular compliance challenges. They may lack specialized privacy officers, cyber-security teams, or legal counsel. A risk-based implementation strategy is therefore preferable to a purely formalistic one. Supervisory guidance can provide model records of processing, simplified impact-assessment templates, breach-response checklists, standard contractual clauses, and sector-specific examples. Such tools lower compliance costs while preserving accountability. The goal should not be to exempt smaller actors from fundamental rights, but to make compliance requirements understandable, proportionate, and operational.

The AI-Specific Implementation Gap: Profiling, Biometrics, Model Training, and Automated Decisions

The title of the present study places the PDP Law in the AI era because AI changes the scale, speed, and opacity of personal-data processing. Four issues are particularly important: profiling, biometric processing, model training, and automated decision-making. Profiling can transform ordinary activity data into predictions about creditworthiness, preferences, health risks, reliability, purchasing power, or likely behavior. Such inferences may influence opportunities even when the underlying data are factually accurate. Data-protection implementation therefore needs to recognize that inferred profiles can be as consequential as the original records from which they were generated.

Biometric processing presents a second high-risk area. Facial recognition, voice recognition, gait analysis, and other biometric systems can identify or classify individuals at scale. Under the PDP Law, biometric data are specific personal data, which signals the need for stronger safeguards. In practice, controllers should demonstrate necessity and proportionality, limit function creep, secure biometric templates, define retention periods, and assess the consequences of false matches or demographic performance disparities. Unlike passwords, biometric characteristics may be difficult or impossible to replace after compromise. This creates a stronger case for privacy by design and for limiting collection where less intrusive authentication methods are sufficient.

Model training presents a third challenge because data may be collected at one stage and reused later to improve algorithmic systems. The legal questions include whether the new purpose is compatible with the original purpose, whether a valid legal basis exists, whether data have been sufficiently minimized or anonymized, and whether data-subject rights can be implemented after training. Meurisch and Mühlhäuser (2021) demonstrate that technical privacy measures must be integrated with governance controls, while Villaronga et al. (2018) show that deletion rights become technically complex where AI systems can retain information in learned representations. The Indonesian framework should therefore encourage documented assessments of training datasets, data provenance, retention, deduplication, access restrictions, and procedures for responding to deletion or objection requests.

Automated decision-making is the most explicit point of contact between AI and the PDP Law. Article 10 provides a right to object to solely automated decisions that have legal or significant effects. The phrase 'significant effect' should be interpreted in a way that captures decisions concerning employment, lending, insurance, education, access to essential services, or other meaningful opportunities. Bayamlioglu (2022) argues that the right to contest automated decisions should be understood beyond a narrow 'right to explanation' and should include effective procedural control. For Indonesian implementation, this supports requirements for notification that automation is being used,

an intelligible description of relevant factors, correction of inaccurate inputs, access to meaningful human review, and documentation showing why the final decision was justified.

The comparison with the GDPR is useful but should be applied carefully. Indonesia's legal and institutional context differs from the European Union. The objective is therefore not regulatory transplantation, but functional learning. GDPR implementation demonstrates that general principles such as accountability, purpose limitation, data minimization, security, and rights of access require detailed organizational systems. Tikkinen-Piri et al. (2018) identified resource and process implications for data-intensive companies, and the same logic applies to Indonesian AI users. A hospital deploying predictive analytics, a bank using automated fraud detection, or a public agency using identity-matching technology needs internal governance proportionate to the consequences of the processing.

AI also raises a fairness question that is not exhausted by privacy. A model can be secure, use lawfully obtained data, and still produce systematically unequal outcomes. Van Bekkum and Zuiderveen Borgesius (2023) discuss the paradox that testing for discrimination can require sensitive attributes that data-protection law restricts. Indonesian implementation should therefore coordinate data-protection requirements with broader anti-discrimination, consumer-protection, administrative-law, and sectoral obligations. Data protection can provide a foundational layer through transparency, accuracy, accountability, minimization, and contestability, but it should not be expected to resolve every problem of algorithmic fairness on its own.

These AI-specific risks reinforce the importance of impact assessment. For high-risk processing, organizations should document the purpose of the AI system, categories and sources of data, lawful basis, necessity, potential harms, security controls, retention, third-party access, bias and accuracy risks, human oversight, and mechanisms for exercising rights. Although the precise legal form of such assessments may depend on implementing regulations and sectoral rules, the underlying practice follows directly from the PDP Law's accountability and security principles. It also creates evidence that can be reviewed by management, auditors, regulators, and courts when a dispute occurs.

Strengthening Implementation: an Integrated Legal and Governance Agenda

The findings support an integrated reform agenda rather than a single solution. First, supervisory capacity must be strengthened. The authority responsible for personal-data protection should have clear jurisdiction, sufficient independence, technical expertise, stable resources, transparent procedures, and the ability to coordinate with sectoral regulators and law-enforcement institutions. Widiatedja and Mishra (2023) and Neta et al. (2022) provide strong support for institutional arrangements that prevent fragmented supervision. For public legitimacy, the authority should also publish accessible guidance and, where legally permissible, anonymized enforcement outcomes so that organizations can understand how abstract statutory principles are applied.

Second, implementing rules and guidance should clarify high-impact rights and duties. Priority areas include automated decision-making and profiling, data-subject requests, compensation, breach notification, data-protection officers, cross-border transfers, controller-processor relationships, and the calculation of administrative sanctions. Clarity does not mean reducing the law to rigid checklists. Rather, it means creating predictable procedures through which principles can be applied consistently. The survey's high uncertainty regarding deterrence and complaint accessibility suggests that procedural visibility is as important as substantive legal language.

Third, controllers should adopt privacy by design and accountability by default. New digital systems should be evaluated before deployment, not only after a breach occurs. Data minimization, access control, logging, encryption, secure retention, deletion procedures, and rights-management interfaces should be part of system architecture. For AI, governance should additionally address training-data provenance, model documentation, automated-decision review, bias testing where lawful and appropriate, and meaningful human oversight. This approach reduces the conflict between innovation and compliance because privacy requirements become engineering and governance criteria from the beginning rather than emergency corrections after harm.

Fourth, public digital literacy must be expanded. The questionnaire shows that awareness exists but is incomplete, while perceptions of government socialization remain divided. Public education should therefore explain practical rights in plain language and through realistic scenarios: what to do after a data breach, how to recognize excessive data requests, how to withdraw consent, how to request access or deletion, how to challenge an automated decision, and where to submit a complaint. Education

should be integrated into schools, universities, public-service communication, professional training, and community digital-literacy programs. In the AI era, literacy must also include an understanding that predictions and profiles can be generated from seemingly ordinary data.

Fifth, organizational compliance should be supported through sector-specific implementation. Risks differ across banking, health, education, employment, telecommunications, e-commerce, and government services. Kholis (2025) demonstrates the importance of cyber-security readiness in banking, while Mayasari (2023) shows that emerging digital environments generate new privacy challenges. Sectoral guidance can translate the PDP Law's general principles into operational requirements without fragmenting the core national standard. Coordination between the central data-protection authority and sector regulators is therefore essential.

Sixth, enforcement should be proportionate but credible. The objective of sanctions is not merely punishment; it is to change incentives and establish a culture of accountability. Regulators should distinguish between good-faith organizations that promptly report and remediate incidents and actors that deliberately exploit data, conceal violations, or repeatedly ignore compliance duties. Transparent sanctioning criteria can improve deterrence because organizations are better able to anticipate the consequences of non-compliance. Criminal law should remain available for conduct that meets statutory elements, while administrative enforcement can respond more flexibly to governance and compliance failures.

Finally, research and evaluation should continue after implementation reforms. Future studies should use larger and more diverse samples, distinguish public and private-sector experiences, measure actual use of data-subject rights, and examine enforcement outcomes. AI-specific empirical research should evaluate how Indonesian organizations apply Article 10 in credit scoring, recruitment, biometric identification, platform moderation, insurance, and public administration. This evidence will be necessary to determine whether the law remains technologically adaptive and whether implementing regulations adequately protect individuals as automated systems become more deeply embedded in everyday decision-making.

CONCLUSION

Law No. 27 of 2022 has established a substantially stronger and more integrated foundation for personal-data protection in Indonesia. It recognizes personal data as an object of legal protection, defines rights of data subjects, regulates the responsibilities of controllers and processors, provides remedies and sanctions, and expressly acknowledges the risk of solely automated decision-making and profiling. The empirical findings, however, show that normative strength has not yet produced uniformly perceived effectiveness. Although 65.3% of respondents reported understanding their data-subject rights, only 38.8% felt more protected after the law's enactment, 28.6% considered complaint mechanisms easy to access, and 30.6% regarded implementation as effective overall. High levels of uncertainty concerning socialization, sanctions, and effectiveness further indicate that institutional visibility and practical enforcement remain central challenges. In the AI era, these weaknesses become more significant because personal data are processed at greater scale and can be transformed into biometric identifiers, behavioral profiles, predictions, and consequential automated decisions. Effective implementation therefore requires an integrated approach: strong and credible supervision, clear implementing procedures, accessible complaints and remedies, organizational accountability, privacy-by-design and cyber-security safeguards, AI impact assessment, meaningful human review of consequential automated decisions, and sustained public digital-literacy programs. The law provides an important legal foundation, but its long-term legitimacy will depend on whether individuals can exercise their rights in practice and whether organizations can demonstrate accountable data governance as technology continues to evolve.

REFERENCES

- Bayamlioglu, E. (2022). The right to contest automated decisions under the General Data Protection Regulation: Beyond the so-called 'right to explanation'. *Regulation & Governance*, 16(4), 1058–1078. <https://doi.org/10.1111/rego.12391>
- European Parliament & Council of the European Union. (2016). *Regulation (EU) 2016/679 of the European Parliament and of the Council (General Data Protection Regulation)*. *Official Journal of the European Union*, L 119, 1–88.

- Kholis, I. M. (2025). Perlindungan data pribadi dan keamanan siber di sektor perbankan: Studi kritis atas penerapan UU PDP dan UU ITE di Indonesia. *Staatsrecht: Jurnal Hukum Kenegaraan dan Politik Islam*, 4(2), 275–299. <https://doi.org/10.14421/t5sfe747>
- Kurniawan, K. D., Hehanussa, D. J. A., Setiawan, R., Susilowati, I., Sopian, & Helfisar, D. (2024). Criminal sanctions and personal data protection in Indonesia. *Lex Publica*, 11(2), 221–247. <https://doi.org/10.58829/lp.11.2.2024.255>
- Manurung, E. A. P. (2023). The right to privacy based on the Law of the Republic of Indonesia Number 27 of 2022. *Journal of Digital Law and Policy*, 2(3), 103–110. <https://doi.org/10.58982/jdlp.v2i3.287>
- Mayasari, H. (2023). A examination on personal data protection in metaverse technology in Indonesia: A human rights perspective. *Journal of Law, Environmental and Justice*, 1(1), 64–85. <https://doi.org/10.62264/jlej.v1i1.4>
- Meurisch, C., & Mühlhäuser, M. (2021). Data protection in AI services: A survey. *ACM Computing Surveys*, 54(2), Article 40, 1–38. <https://doi.org/10.1145/3440754>
- Neta, Y., Awanisa, A., & Melisa. (2022). The urgency of independent supervisory authority towards Indonesia's personal data protection. *Constitutionale*, 3(1), 21–42. <https://doi.org/10.25041/constitutionale.v3i1.2535>
- Republic of Indonesia. (2022). *Law of the Republic of Indonesia Number 27 of 2022 concerning Personal Data Protection*. State Gazette of the Republic of Indonesia No. 196 of 2022.
- Rinjani, M. A., & Firmansyah, R. (2025). Hambatan implementasi UU 27/2022 dan strategi penguatan perlindungan data pribadi di Indonesia. *Jurnal Analisis Hukum*, 8(1), 70–83. <https://doi.org/10.38043/jah.v8i1.6793>
- Simbolon, V. A., & Juwono, V. (2022). Comparative review of personal data protection policy in Indonesia and the European Union General Data Protection Regulation. *Publik (Jurnal Ilmu Administrasi)*, 11(2), 178–190. <https://doi.org/10.31314/pjia.11.2.178-190.2022>
- Soemitro, D. P., Wicaksono, M. A., & Putri, N. A. (2023). Penal provisions in the Personal Data Protection Law: A comparative legal study between Indonesia and Singapore. *SIGn Jurnal Hukum*, 5(1), 155–167. <https://doi.org/10.37276/sjh.v5i1.272>
- Tikkinen-Piri, C., Rohunen, A., & Markkula, J. (2018). EU General Data Protection Regulation: Changes and implications for personal data collecting companies. *Computer Law & Security Review*, 34(1), 134–153. <https://doi.org/10.1016/j.clsr.2017.05.015>
- van Bekkum, M., & Zuiderveen Borgesius, F. (2023). Using sensitive data to prevent discrimination by artificial intelligence: Does the GDPR need a new exception? *Computer Law & Security Review*, 48, 105770. <https://doi.org/10.1016/j.clsr.2022.105770>
- Villaronga, E. F., Kieseberg, P., & Li, T. (2018). Humans forget, machines remember: Artificial intelligence and the right to be forgotten. *Computer Law & Security Review*, 34(2), 304–313. <https://doi.org/10.1016/j.clsr.2017.08.007>
- Widiatedja, I. G. N. P., & Mishra, N. (2023). Establishing an independent data protection authority in Indonesia: A future-forward perspective. *International Review of Law, Computers & Technology*, 37(3), 252–273. <https://doi.org/10.1080/13600869.2022.2155793>
- Wiwoho, J., Pati, U. K., & Pratama, A. M. (2024). Reciprocal data portability to foster financial services competition in the open banking system era. *Yustisia*, 13(2), 134–150. <https://doi.org/10.20961/yustisia.v13i2.75786>
- Yusliwidaka, A., Abqa, M. A. R., & Wardana, K. A. (2024). A discourse of personal data protection: How Indonesia responsible under domestic and international law? *Pandecta Research Law Journal*, 19(2), 453–482. <https://doi.org/10.15294/pandecta.v19i2.13279>