International Journal of Law, Policy and Social Review
www.lawjournals.net
Online ISSN: 2664-6838
Received: 24-03-2026, Accepted: 24-04-2026, Published: 09-05-2026
Volume 8, Issue 2, 2026, Page No. 148-155

# The politics of personal data protection law in indonesia in safeguarding privacy rights in the era of digital transformation

**Rezky Muliamarta[1], Dr. Bambang Slamet Riyadi[2], Dr. Riza Zulfikar[2]**
[1] Faculty of Law, Langlangbuana University, Bandung, West Java, Indonesia
[2] Lecturer, Master of Law, Postgraduate Program Langlangbuana University Bandung, West Java, Indonesia
**Correspondence Author:** Rezky Muliamarta

**Abstract**
The rapid acceleration of digital transformation has fundamentally reshaped social interaction, economic transactions, and governmental administration in Indonesia. The growing dependence on digital systems has significantly increased the collection, storage, processing, and dissemination of personal data by both public institutions and private corporations. While digitalisation offers efficiency, innovation and economic opportunities, it simultaneously creates substantial legal risks, including privacy violations, identity theft, data breaches, unauthorised profiling and weak regulatory enforcement. This research aims to analyse the politics of law underlying the enactment of Law Number 27 of 2022 concerning Personal Data Protection and to assess its role in safeguarding citizens' privacy rights. This study employs a normative juridical method using statutory, conceptual, and comparative approaches. The findings indicate that the enactment of the
Personal Data Protection Law reflects the State's legal policy in strengthening constitutional rights protection amid digital transformation. Nevertheless, fragmented regulations, institutional limitations, low compliance culture and rapid technological innovation remain major challenges. Therefore, institutional strengthening, regulatory harmonisation and the enhancement of public digital literacy are essential to ensure effective implementation.

**Keywords:** Politics of law, personal data protection, privacy rights, digital transformation, indonesia

## Introduction

The rapid development of information and communication technology over the last two decades has generated profound changes in modern society, including in Indonesia. The internet, smartphones, cloud computing, artificial intelligence and integrated digital systems have transformed the manner in which individuals work, communicate, conduct transactions and access public services. Digital transformation is no longer perceived as a supplementary phenomenon; rather, it has become an integral component of contemporary social and economic structures.

Indonesia, as one of the most populous countries in the world and one of the largest digital markets in Southeast Asia, has experienced substantial growth in digital activity. Electronic commerce, digital banking, online transportation services, social media platforms, e-learning systems and e-government initiatives have expanded rapidly in recent years. These developments demonstrate that Indonesia's economy and public administration are increasingly dependent upon digital infrastructure.

Within the modern digital ecosystem, data constitutes a central strategic asset. Nearly every digital interaction generates information. Whenever an individual opens an application, purchases goods online, books transportation, accesses healthcare services, participates in online education, or uses social media, digital systems record multiple forms
of data. Such information may include names, addresses, telephone numbers, geolocation records, consumption patterns, behavioural preferences, financial records and biometric identifiers.

Consequently, personal data has undergone a significant conceptual transformation. Previously regarded merely as administrative information, personal data has now become a valuable economic asset. Numerous technology companies develop business models based upon the large-scale collection and processing of user information. In many contemporary discussions, data has even been characterised as the "new oil" of the digital economy due to its strategic commercial value.

However, the increasing economic value of personal data has also generated serious risks of misuse. Excessive data collection, unauthorised sharing, hidden profiling practices, commercial exploitation without consent and large-scale data breaches have become significant threats to citizens. In many instances, individuals remain in a structurally weaker position because they are unable to understand how their data is collected, processed, stored or transferred.

Indonesia has experienced several high-profile incidents involving alleged data leaks affecting both private corporations and public institutions. Such incidents have generated public concern because data that should have been legally protected became vulnerable to fraud, identity theft, cybercrime and other unlawful exploitation. Beyond material losses, these incidents also undermine public trust in national digital systems.

Public trust is, in fact, one of the essential foundations of a sustainable digital economy. Without confidence that personal information will be handled responsibly and securely, citizens may become reluctant to engage with digital services. Such reluctance may ultimately hinder innovation, digital investment and the broader modernisation of public services.

From a legal perspective, the issue of personal data protection is not merely technological in nature. It is closely connected to human rights, constitutional guarantees and the dignity of individuals. Privacy enables persons to retain control over information concerning themselves and to maintain autonomy against arbitrary intrusion.

The Indonesian Constitution provides an important normative basis for such protection. Article 28G paragraph (1) of the 1945 Constitution of the Republic of Indonesia guarantees every person the right to personal protection, family protection, honour, dignity, property and security from threats of fear. This constitutional provision may reasonably be interpreted as encompassing the protection of personal data as an extension of personal security and dignity.

The philosophical foundation of the Unitary State of the Republic of Indonesia is Pancasila, with its principles formulating the abstract principles or essence of Indonesian human life, which are based on three complete relationships of human nature: the relationship between humans and God, the relationship between humans, including themselves, and the relationship between humans and objects (including inorganic, vegetative and animal objects). The Fifth principle, provides direction for the growth of awareness of each individual as a social being – who upholds justice together with others as fellow citizens.

Nevertheless, Indonesia long lacked a single comprehensive legal instrument specifically governing personal data protection. Prior to the enactment of Law Number 27 of 2022 concerning Personal Data Protection (hereinafter PDP Law), relevant norms were scattered across various sectoral regulations, including the Electronic Information and Transactions Law, telecommunications regulations, banking law, healthcare law and population administration law.

Such fragmented regulation generated several structural problems. First, there was no unified legal standard concerning the definition of personal data, lawful consent, rights of data subjects or obligations of data controllers. Second, enforcement mechanisms were dispersed across different institutions. Third, individuals often faced difficulty obtaining remedies when their rights were violated. As a consequence, legal certainty in the field of personal data protection remained weak.

The enactment of the PDP Law in 2022 marked an important milestone in Indonesian legal development. It signified formal recognition by the State that personal data constitutes a legal interest requiring comprehensive statutory protection. The law also reflects Indonesia's response to global legal developments, as many jurisdictions have already adopted modern data protection regimes.

However, the mere enactment of legislation does not automatically resolve practical problems. The real challenge lies in implementation. Law enforcement capacity, institutional readiness, corporate compliance, public legal awareness and the rapid evolution of technology are all decisive factors affecting the effectiveness of the PDP Law.

From the perspective of politics of law, every statute represents a deliberate policy choice of the State. Through legislation, the State determines which values should be protected, whose interests should be prioritised and what direction national legal development should take. Accordingly, the PDP Law should be analysed not merely as a legal text, but as a product of national legal policy.

Furthermore, a gap remains between das sollen (normative expectations) and das sein (empirical reality). Normatively, citizens possess rights to privacy and data protection. Empirically, however, data leaks, misuse of information and weak enforcement continue to occur. This discrepancy demonstrates the importance of conducting a deeper legal analysis regarding Indonesia's politics of law in the area of personal data protection.

This research is increasingly relevant because personal data will become even more strategic in the future. The rise of artificial intelligence, the Internet of Things, biometric systems, integrated databases and cross-border digital services will intensify the need for adaptive legal protection. The State must therefore strike an appropriate balance between technological innovation, economic growth and the protection of citizens' fundamental rights.

Based on the foregoing background, this article examines the politics of law underlying the enactment of the PDP Law, the obstacles to its implementation and future models of legal reform aimed at safeguarding privacy rights in Indonesia during the era of digital transformation.

**Research Questions**

Based on the background outlined above, this study addresses the following legal questions:

1. What politics of law underlies the enactment of Law Number 27 of 2022 concerning Personal Data Protection in Indonesia?
2. What are the principal challenges in implementing personal data protection in safeguarding citizens' privacy rights?
3. What model of future legal reform should be developed to strengthen personal data protection in Indonesia?

**Research Method**

This study employs a normative juridical research method, focusing primarily on positive legal norms, legal principles, legal doctrines and the harmonisation of statutory regulations. A normative approach is appropriate because the principal object of this study concerns legislative policy, constitutional protection and legal construction in the field of personal data protection.

The approaches used in this research are as follows:

**1. Statutory Approach**

This approach examines relevant legislation, including:

1. The 1945 Constitution of the Republic of Indonesia;
2. Law Number 27 of 2022 concerning Personal Data Protection;
3. The Electronic Information and Transactions Law and its amendments;
4. Government Regulation Number 71 of 2019 concerning the Operation of Electronic Systems and Transactions.

**2. Conceptual Approach**

This approach applies relevant legal theories and concepts, including:

- Rule of law theory;
- Legal protection theory;
- Privacy rights theory;
- Politics of law theory;
- Constitutional rights doctrine.

**3. Comparative Approach**

This approach compares Indonesian law with foreign legal regimes, particularly:

- The European Union General Data Protection Regulation (GDPR);
- Singapore Personal Data Protection Act;
- Malaysia Personal Data Protection Act.

**4. Sources of Legal Materials**

The study uses:

- **Primary legal materials:** statutes and regulations;

- **Secondary legal materials:** books, journals, scholarly writings, expert opinions;
- **Tertiary legal materials:** legal dictionaries and encyclopaedias.

**5. Analytical Method**

All legal materials are analysed qualitatively through descriptive-analytical methods in order to identify the direction of Indonesia's politics of law in the field of personal data protection.

**Discussion**

**a. The Politics of Law Behind the Enactment of the Personal Data Protection Law in Indonesia**

The enactment of legislation is never a value-neutral process. Every statute emerges from a combination of political considerations, social demands, economic developments, institutional pressures and the broader direction of state policy. In this context, Law Number 27 of 2022 concerning Personal Data Protection (hereinafter the PDP Law) should be understood not merely as a technical regulatory instrument, but as an expression of Indonesia's politics of law in responding to digital transformation.

Moh. Mahfud MD defines politics of law as the official policy of the State concerning laws that will be enacted, amended, maintained or repealed in order to achieve the objectives of the nation. Based on this conception, the PDP Law represents a conscious legal policy choice by the Indonesian State to place personal data protection within the category of strategic national interests.

Prior to the enactment of the PDP Law, Indonesia did not possess a unified legal regime specifically regulating personal data protection. Relevant norms were dispersed across numerous sectoral laws and regulations, including the Electronic Information and Transactions Law, population administration law, banking law, healthcare regulations, consumer protection rules and ministerial regulations. Such fragmentation created uncertainty regarding the rights of individuals, the obligations of data processors and the mechanisms of enforcement.

The absence of a comprehensive framework generated several structural weaknesses. First, there was no harmonised definition of personal data and no single standard regarding lawful consent, retention periods, data transfer or accountability. Second, supervisory authority was institutionally dispersed. Third, citizens whose data had been misused often lacked accessible remedies. As a result, legal certainty in this field remained underdeveloped.

From the perspective of politics of law, this situation demonstrates a common challenge faced by many developing legal systems: technological change progressed faster than legislative adaptation. Indonesian society had already entered an era of e-commerce, digital finance, platform economies, biometric systems and data-driven governance, while the legal framework remained largely sectoral and reactive.

The enactment of the PDP Law was also strongly influenced by rising public concern over data breach incidents. Several high-profile cases involving alleged leaks of customer information, user databases and public-sector data heightened awareness regarding the vulnerability of digital systems. These events generated public pressure for the State to adopt stronger legal safeguards.

Beyond domestic concerns, international developments also played an important role. Many jurisdictions had already established advanced personal data protection regimes. The European Union's General Data Protection Regulation (GDPR), in particular, became a global benchmark influencing trade relations, investment confidence and cross-border data transfers.

In the global digital economy, data protection is no longer solely a matter of civil liberties; it is also connected to economic competitiveness. Countries lacking credible data governance frameworks may encounter obstacles in attracting digital investment, participating in international technology markets and securing cooperation with foreign enterprises.

Accordingly, the PDP Law may be viewed as part of Indonesia's broader economic strategy. By strengthening legal certainty in data governance, the State seeks to build public trust, encourage digital innovation, attract investment and integrate Indonesia more effectively into global digital markets.

The law also reflects a normative shift in how the State conceptualises personal data. Previously, personal data was often treated as administrative information managed by institutions. Under the modern approach embodied in the PDP Law, personal data is recognised as an extension of individual autonomy and dignity. This conceptual shift is highly significant because it changes the orientation of legal protection from institution-centred governance to rights-centred governance.

The PDP Law recognises multiple rights of data subjects, including the right to obtain information, the right to access data, the right to rectify inaccurate data, the right to withdraw consent, the right to delay or restrict certain processing and the right to seek compensation for violations. These provisions indicate that individuals are no longer passive objects of data collection but legal subjects possessing enforceable rights.

Nevertheless, the legislative process also reflects the balancing of competing interests. As with many modern regulatory frameworks, the PDP Law emerged through negotiation among state institutions, digital industry actors, civil society organisations and policy makers. The State had to reconcile several objectives simultaneously: protecting privacy rights, supporting digital economic growth, facilitating public-sector efficiency and maintaining regulatory feasibility.

Thus, the politics of law behind the PDP Law can be understood as resting upon three principal foundations. First, the constitutional obligation to protect citizens' rights. Second, the economic necessity of building a trusted digital ecosystem. Third, the strategic need to harmonise Indonesian law with global legal standards.

**b. Privacy as a Constitutional Right within the Indonesian Legal System**

Privacy is one of the fundamental values of modern constitutional democracies. It provides individuals with a protected sphere in which they may control personal information, maintain dignity, develop relationships and exercise autonomy free from arbitrary interference. In contemporary legal theory, privacy is no longer understood merely as secrecy; rather, it is closely linked to liberty, identity and human dignity.

Historically, threats to privacy were largely physical in nature, such as unlawful searches, surveillance of correspondence or direct intrusion into private spaces. In the digital era, however, the nature of privacy threats has changed dramatically. Technology now enables the large-scale collection, aggregation, storage, analysis and commercialisation of personal information with unprecedented speed and precision.

Digital platforms can infer behavioural tendencies, psychological preferences, purchasing habits, social relationships, geographic movement and political inclinations through algorithmic analysis. In this environment, the loss of control over personal data often equates to the erosion of privacy itself.

For this reason, personal data protection should be understood as a contemporary legal manifestation of privacy protection. When an individual cannot determine who accesses their information, how it is processed or for what purposes it is used, that person loses a significant dimension of personal autonomy.

Philosophically, privacy derives from respect for the person as an autonomous moral agent. Every individual should possess the freedom to decide what information about themselves is disclosed, to whom it is disclosed and under what conditions it may be used. Without such control, persons risk being reduced to objects of economic exploitation, political manipulation or bureaucratic administration.

Within the Indonesian constitutional framework, although the term "privacy" is not expressly stated in a single comprehensive clause, its substance is clearly embedded in several constitutional provisions. Article 28G paragraph (1) of the 1945 Constitution guarantees every person the right to personal protection, family protection, honour, dignity, property and security from threats of fear.

This provision provides a strong normative basis for recognising privacy and personal data protection as constitutional interests. Personal data represents the identity of the individual. Misuse of such data may jeopardise dignity, safety, economic wellbeing and personal reputation.

Furthermore, Article 28D paragraph (1) of the Constitution guarantees the right to recognition, guarantees, protection and fair legal certainty. In the digital context, this provision requires the State to establish a clear legal framework governing the collection and processing of personal data.

Privacy also bears a close relationship to freedom of thought and freedom of expression. Individuals who believe that every action, communication or digital interaction is continuously monitored may become reluctant to express opinions, explore ideas or participate freely in democratic discourse. Thus, privacy is not opposed to democracy; rather, it is one of democracy's enabling conditions.

International human rights law reinforces this constitutional interpretation. Article 12 of the Universal Declaration of Human Rights (UDHR) and Article 17 of the International Covenant on Civil and Political Rights (ICCPR) prohibit arbitrary interference with privacy, family, home and correspondence. As a member of the international community and a party to major human rights instruments, Indonesia carries both moral and legal responsibilities to align domestic law with these standards.

Large-scale data breaches may therefore be understood not merely as technical failures, but as infringements upon constitutional rights. When identity numbers, addresses, health information, financial records or biometric data are exposed without authorisation, individuals may suffer fraud, extortion, discrimination, reputational harm and economic loss.

In constitutional terms, the State cannot remain passive. Human rights doctrine generally recognises three principal state obligations: to respect rights, to protect rights from third-party interference and to fulfil rights through positive measures. Applied to privacy, these obligations require the State to refrain from arbitrary misuse of data, prevent abuse by private actors and establish effective remedies for victims.

The enactment of the PDP Law can be interpreted as part of Indonesia's effort to fulfil these constitutional duties. Through the law, the State creates rights for data subjects while imposing duties upon controllers and processors.

However, constitutional protection must exist in practice, not only in legislation. If data breaches remain frequent, oversight remains weak and victims cannot secure remedies, then privacy protection risks becoming symbolic rather than substantive.

Accordingly, privacy within the Indonesian legal system should be recognised as a constitutional right requiring active state protection. Personal data protection is one of the most important legal instruments through which that right may be realised in the era of digital transformation.

### c. Challenges in the Implementation of the Personal Data Protection Law in Indonesia

The enactment of Law Number 27 of 2022 concerning Personal Data Protection represents a significant milestone in Indonesia's legal development. However, the effectiveness of any legislation depends not solely upon the quality of its normative provisions, but upon its practical implementation. In Lawrence M. Friedman's theory of the legal system, the functioning of law is determined by three interrelated components: legal structure, legal substance and legal culture. Accordingly, the implementation of the PDP Law must be examined through a multidimensional lens.

#### 1. Institutional and Supervisory Challenges

One of the most decisive elements in any personal data protection regime is the existence of a competent and independent supervisory authority. In many jurisdictions, data protection law is enforced through specialised agencies empowered to receive complaints, conduct investigations, impose administrative sanctions, issue compliance guidelines and monitor systemic risks.

Indonesia continues to face challenges concerning institutional design and enforcement capacity. Without a strong supervisory body, the rights recognised under the PDP Law may remain largely declaratory. Citizens may formally possess rights to privacy and data protection, yet lack effective institutional avenues through which those rights can be defended.

An independent authority is particularly important in balancing structural inequalities between individuals and large digital corporations. Major technology companies often possess superior legal resources, technical expertise and financial capacity compared with ordinary users. Therefore, state intervention through a credible regulator is essential to preserve fairness and accountability.

Coordination among ministries and state agencies also remains a challenge. Personal data governance intersects with banking, healthcare, taxation, telecommunications,

education, population administration, social welfare and law enforcement. Without clear institutional coordination, overlapping authority and inconsistent regulatory standards may emerge.

**2. Low Compliance Among Electronic System Operators**

A second challenge concerns the compliance culture of electronic system operators in both the public and private sectors. Many organisations collect vast quantities of personal information without implementing robust governance systems or sufficient cybersecurity safeguards.

Common problems include:

- unclear or inaccessible privacy notices;
- consent mechanisms designed merely as formalities;
- excessive data collection beyond operational necessity;
- weak internal security controls;
- delayed breach notifications;
- inadequate employee training regarding data governance.

For some businesses, data protection is still perceived as an additional cost rather than a legal obligation and reputational investment. This perception is problematic because in the digital economy, trust constitutes a valuable commercial asset. Companies that fail to safeguard user information risk losing public confidence, market share and legal legitimacy.

The same concern applies to public institutions. Government bodies process highly sensitive data relating to population records, taxation, healthcare, education, social assistance and public services. A data breach in the public sector may affect millions of citizens simultaneously and can produce severe consequences for national trust in governance systems.

**3. Limited Digital Literacy and Public Legal Awareness**

The implementation of the PDP Law does not depend solely on regulators and corporations. Citizens themselves play a crucial role as data subjects. Indonesia still faces substantial challenges in terms of digital literacy and public understanding of privacy rights.

Many users continue to disclose personal information to unverified applications, overshare identity details on social media, click malicious links or provide verification codes to fraudulent actors. Numerous individuals remain unaware that personal data possesses economic value and may be exploited for criminal or manipulative purposes.

As a result, citizens frequently become victims of phishing, identity theft, online fraud, illegal lending schemes, account hijacking and extortion based on leaked personal information. In such circumstances, legal protection often becomes reactive rather than preventive.

A stronger legal culture is therefore necessary. Citizens should understand their rights to:

- know the purpose of data processing;
- refuse unlawful or unnecessary collection;
- request correction of inaccurate information;
- request deletion in certain circumstances;
- object to harmful processing activities;
- seek remedies for misuse of data.
- Without such awareness, rights guaranteed by statute risk remaining dormant.

**4. Technological Development Outpacing Regulation**

One of the recurring difficulties in technology law is that innovation frequently advances faster than legislation. By the time a statute is enacted, new technological practices may already have emerged that were not fully anticipated by lawmakers.

Indonesia, like many other jurisdictions, now faces the rapid expansion of artificial intelligence, machine learning, biometric recognition, blockchain systems, smart devices, predictive analytics and the Internet of Things. These technologies rely heavily upon large-scale data processing.

Artificial intelligence systems, for example, may analyse behavioural patterns in order to predict political preferences, purchasing tendencies, creditworthiness, health risks or employment suitability. If insufficiently regulated, such systems may facilitate algorithmic discrimination, hidden manipulation, opaque automated decision-making or mass surveillance.

The PDP Law provides an important foundational framework, yet future implementation will require adaptive subsidiary regulations and responsive interpretation capable of addressing technological evolution.

**5. Law Enforcement and Remedies for Victims**

Another crucial challenge concerns law enforcement and access to remedies. In many data breach cases, victims suffer genuine losses but encounter serious obstacles in proving responsibility, causation or measurable damage.

Personal data disputes often involve technical evidence, cybersecurity audits, digital forensics, cross-border data flows and complex contractual arrangements. Effective enforcement therefore requires specialised expertise among regulators, investigators, judges and legal practitioners.

Moreover, remedial mechanisms should be simple, affordable and accessible. If individuals must engage in lengthy and expensive litigation merely to protect their privacy, access to justice becomes severely limited.

Collective redress mechanisms may also be relevant. Large-scale breaches frequently affect thousands or millions of users simultaneously. In such circumstances, class actions or representative proceedings may offer more efficient avenues of justice than purely individual claims.

Accordingly, implementation challenges under the PDP Law are not merely normative they are institutional, technological, cultural and procedural in nature.

**d. Comparative Analysis: European Union, Singapore, and Malaysia**

Comparative legal analysis is valuable in assessing Indonesia's position within global regulatory developments and in identifying best practices for future reform. Several jurisdictions have established more mature data protection systems from which important lessons may be drawn.

**1. European Union: General Data Protection Regulation (GDPR)**

The European Union's General Data Protection Regulation is widely regarded as one of the most advanced data protection regimes in the world. Since entering into force in 2018, the GDPR has significantly influenced global compliance standards.

The GDPR places individuals at the centre of protection. It recognises rights such as:

- the right of access;
- the right to rectification;
- the right to erasure ("right to be forgotten");
- the right to data portability;
- the right to object to certain processing;
- the right to be informed of data breaches.

The GDPR also imposes substantial administrative fines, including penalties calculated as percentages of global annual turnover. This enforcement model has incentivised serious corporate compliance efforts.
The principal lesson from the European Union is that data protection requires more than symbolic recognition of rights; it requires credible enforcement, independent regulators and meaningful sanctions.

**2. Singapore: Personal Data Protection Act (PDPA)**
Singapore has developed a comparatively pragmatic and business-oriented model while maintaining clear legal safeguards. The Personal Data Protection Act regulates consent, purpose limitation, security obligations, breach notification and complaint mechanisms.
Singapore's Personal Data Protection Commission plays an active role in issuing guidance, educating organisations and imposing sanctions where necessary. This demonstrates the importance of a responsive regulator capable of combining enforcement with practical compliance support.
For Indonesia, Singapore offers an example of how privacy protection may coexist with a dynamic and innovation-friendly digital economy.

**3. Malaysia: Personal Data Protection Act**
Malaysia was among the earlier Southeast Asian jurisdictions to adopt dedicated personal data protection legislation. Its framework initially focused more strongly on commercial transactions but nonetheless established important principles concerning consent, disclosure and lawful processing.
Malaysia illustrates that data protection systems in developing economies may evolve incrementally in accordance with domestic institutional capacity and economic priorities.

**4. Indonesia's Position**
Through the PDP Law, Indonesia has moved in the right direction by adopting several modern principles, including consent, data subject rights, accountability obligations, administrative sanctions and criminal penalties for serious violations.
However, compared with the European Union and Singapore, Indonesia still faces substantial challenges concerning:
- supervisory institutional strength;
- technical enforcement capacity;
- nationwide compliance readiness;
- public legal literacy;
- harmonisation across sectors.

Indonesia's major advantage lies in timing and scale. With one of the fastest-growing digital economies in the region, the country possesses a valuable opportunity to develop a trusted digital ecosystem supported by credible privacy governance.

**5. Lessons for Indonesia**
Comparative analysis suggests at least five important lessons:
1. Individuals must remain the central subjects of protection.
2. An independent and active supervisory authority is essential.
3. Sanctions must be real and enforceable.
4. Public education and organisational guidance must be continuous.
5. Regulation must remain adaptive to technological change.

Accordingly, successful data protection regimes are built not merely upon legislation, but upon the integration of law, institutions and compliance culture.

**e. Future Model of Legal Reform for Personal Data Protection in Indonesia**
Personal data protection in Indonesia cannot end with the mere enactment of Law Number 27 of 2022 concerning Personal Data Protection. Legislation provides an essential legal foundation, yet effective protection can only be achieved through institutional reform, regulatory harmonisation, enforcement capacity and the development of a strong culture of digital rights awareness. Accordingly, Indonesia's future politics of law must be directed toward building a comprehensive, adaptive and sustainable data protection ecosystem.

**1. Establishment of an Independent Data Protection Authority**
One of the most urgent institutional priorities is the creation and strengthening of an independent supervisory authority responsible for overseeing personal data protection. Comparative experience demonstrates that successful privacy regimes rely upon specialised
bodies capable of receiving complaints, conducting investigations, imposing administrative sanctions, issuing technical guidance and monitoring systemic risks.
Institutional independence is crucial to ensure that enforcement is not influenced by political or commercial interests. A credible authority must possess jurisdiction over both state institutions and private corporations. Without such independence, oversight over public-sector data processing may be compromised.
In addition, the authority should be staffed by experts in law, cybersecurity, information systems, consumer protection and digital governance. Personal data regulation is inherently interdisciplinary and cannot be managed solely through conventional administrative approaches.

**2. Harmonisation of Sectoral Regulations**
Indonesia possesses numerous sector-specific regulations concerning healthcare data, banking secrecy, telecommunications records, taxation information, educational databases and population administration. If these frameworks remain inconsistent, legal uncertainty and normative conflict will persist.
For example, confidentiality standards in banking may differ from those in healthcare or telecommunications. Inter-agency data sharing may also occur without uniform procedural safeguards. In such situations, data subjects bear the greatest risk.
Therefore, future legal policy should position the PDP Law as the principal umbrella framework, while sectoral regulations operate as technical implementing instruments consistent with its fundamental principles. Harmonisation would improve legal certainty, reduce overlapping authority and create clearer compliance standards.

**3. Strengthening Corporate Compliance and Internal Governance**
Digital platforms, financial institutions, hospitals, e-commerce providers, telecommunications operators and

other entities processing personal data should be required to establish robust internal governance mechanisms.
Necessary measures include:

- appointment of data protection officers;
- regular cybersecurity audits;
- privacy-by-design systems;
- data minimisation practices;
- rapid breach notification procedures;
- employee training on data governance responsibilities.

Modern compliance models should not rely solely upon deterrence through sanctions. They must also promote good data governance as a core element of corporate responsibility. In the long term, organisations that demonstrate trustworthy data practices are likely to enjoy stronger reputations and greater commercial sustainability.

**4. Strengthening Enforcement and Access to Remedies**

A sound politics of law must ensure that citizens possess meaningful access to justice when privacy rights are violated. Complaint procedures and dispute resolution mechanisms should therefore be simple, efficient, affordable and technologically accessible.
Victims of data breaches often do not know where to report violations. Even where harm is clear, proving causation and responsibility may be difficult. The State should therefore develop evidentiary and procedural mechanisms suited to digital harms, including the use of forensic evidence and technical audits.
Administrative sanctions should be complemented by civil and criminal liability for serious misconduct, such as unlawful sale of personal data, organised identity theft or intentional misuse of sensitive information.
Furthermore, class actions or representative proceedings should be considered for mass data breach cases affecting large numbers of individuals simultaneously.

**5. Public Digital Literacy and Privacy Education**

Personal data protection cannot function effectively if citizens do not understand the value of their own information. For this reason, public education should become a central pillar of future legal policy.
Digital literacy programmes should educate citizens regarding:

- the importance of safeguarding personal data;
- risks of oversharing identity information;
- understanding privacy notices and consent requests;
- recognising online fraud and phishing;
- using secure authentication methods;
- exercising legal rights against misuse of data.

Such education should begin in schools, universities, workplaces, and public awareness campaigns. Citizens should not merely be users of technology, but informed rights-holders within the digital legal order.

**6. Adaptive Regulation for Emerging Technologies**

Technological innovation will continue to generate new privacy risks. Artificial intelligence, biometric surveillance, smart cities, predictive analytics, blockchain ecosystems and autonomous decision-making systems require forward-looking governance.
Accordingly, Indonesia should adopt periodic regulatory review mechanisms to ensure that legal frameworks remain responsive. Regulatory sandboxes may also be useful in allowing innovation to develop under controlled safeguards.
Future legal debates are likely to focus increasingly on algorithmic accountability, AI bias, automated decision-making transparency and the processing of biometric data.

**7. Regional and International Cooperation**

Personal data routinely moves across national borders. Many digital services used by Indonesian citizens are operated by multinational corporations storing information in multiple jurisdictions. Consequently, national legal policy cannot remain purely domestic in orientation.
Indonesia should strengthen regional ASEAN cooperation and broader international engagement regarding:

- cross-border data transfers;
- cybercrime enforcement cooperation;
- minimum privacy standards;
- exchange of regulatory best practices;
- international consumer protection mechanisms.

Active participation in global digital governance would enhance Indonesia's strategic position while protecting national interests and citizens' rights.

**Conclusion**

Digital transformation has positioned personal data as a central asset in contemporary social, economic and governmental life. In this context, personal data protection is no longer a merely technical issue; it is a constitutional issue directly connected to privacy, human dignity, security and public trust in digital systems.
The enactment of Law Number 27 of 2022 concerning Personal Data Protection represents an important manifestation of Indonesia's politics of law in responding to contemporary challenges. The statute reflects a significant normative shift by recognising personal data as a legal interest closely tied to fundamental rights and deserving comprehensive statutory protection.
Nevertheless, this study demonstrates that major implementation challenges remain. Institutional limitations, inconsistent compliance among electronic system operators, low public digital literacy, limited access to remedies and the rapid evolution of technology all continue to hinder the effectiveness of personal data protection in Indonesia.
Comparative analysis of the European Union, Singapore, and Malaysia indicates that successful data protection regimes depend upon the integration of clear legal norms, independent supervisory institutions, effective sanctions, public awareness and adaptive governance.
Accordingly, Indonesia's future politics of law should focus not merely on preserving statutory provisions, but on building a functioning ecosystem of privacy protection. The State must ensure that every citizen can enjoy meaningful protection of personal data in everyday digital life.

**Recommendations**

Based on the findings of this study, the following recommendations are proposed:

1. The Government should promptly establish and strengthen an independent personal data protection authority with adequate legal powers and technical capacity.
2. Sectoral regulations involving data governance should be harmonised with the principles of the PDP Law.

3. Public and private electronic system operators should be required to implement robust security standards and regular compliance audits.
4. Nationwide digital literacy programmes should be developed to improve awareness of privacy rights and cybersecurity risks.
5. Complaint mechanisms, dispute resolution procedures, and compensation systems for victims of data breaches should be made faster, simpler and more accessible.
6. Future regulations should be developed to address artificial intelligence, biometric technologies and emerging forms of automated data processing.
7. Indonesia should strengthen regional and international cooperation concerning cross-border data governance and cyber enforcement.

**References**


1. Bennett CJ. Regulating Privacy: Data Protection and Public Policy in Europe and the United States. Cornell University Press, 1992.
2. Castells M. The Rise of the Network Society. Wiley-Blackwell, 2010.
3. Constitution of the Republic of Indonesia, 1945.
4. Friedman LM. The Legal System: A Social Science Perspective. Russell Sage Foundation, 1975.
5. Greenleaf G. Asian Data Privacy Laws. Oxford University Press, 2014.
6. Hildebrandt M. Law for Computer Scientists and Other Folk. Oxford University Press, 2020.
7. Hildebrandt M. Smart Technologies and the End(s) of Law. Edward Elgar, 2015.
8. International Covenant on Civil and Political Rights 1966, 1966.
9. Law Number 27 of 2022 concerning Personal Data Protection, 2022.
10. Mahfud MD M. Politik Hukum di Indonesia. Rajawali Pers, 2017.
11. Marzuki PM. Legal Research. Kencana, 2021.
12. Mayer-Schönberger V, Cukier K. Big Data. John Murray Publishers, 2013.
13. OECD. Digital Economy Outlook. OECD Publishing, 2020.
14. OECD. Government at a Glance: Digital Government. OECD Publishing, 2021.
15. OECD. Privacy Guidelines. OECD Publishing, 2013.
16. Rahardjo S. Law and Social Change. Genta Publishing, 2009.
17. Regulation (EU) 2016/679 (General Data Protection Regulation), 2016.
18. Rosadi SD. Cyber Law: Perlindungan Privasi atas Data Pribadi dalam Era Ekonomi Digital. Refika Aditama, 2018.
19. Rotenberg M. Privacy Law Sourcebook. EPIC, 2020.
20. Schwartz PM, Solove DJ. Information Privacy Law. Wolters Kluwer, 2021.
21. Shue H. Basic Rights. Princeton University Press, 1980.
22. Singapore Personal Data Protection Act, 2012.
23. Siswanto, Riyadi BS. Criminal Court Decisions On the Deterrent Effect In Indonesia, 2026, 8(1).
24. Solove DJ. Understanding Privacy. Harvard University Press, 2008.
25. Universal Declaration of Human Rights. 1948.