The Legal Reform of The Independent Supervisory Institution for The Enforcement of Personal Data Protection Law

Bachtiar Noprianto[1,*], *Tina* Amelia[1]

[1] Faculty of Law, Borobudur University, Indonesia

Abstract. Indonesia lacks a dedicated institution for personal data protection, a lack of which has led to increased data breaches and misuse. The Presidential Regulation, which regulates duties and authorities, has not been effective in addressing the issue. The country's transition to digital technologies has not led to comprehensive legal protections. This type of research uses normative juridical research methods, using a statutory approach and an analytical approach, with the primary legal material is Law No. 27 of 2022 on the Protection of Personal Data, followed by analysis through grammatical interpretation and teleological interpretation. The result suggests that In Indonesia, the responsibility for overseeing data protection is currently held by an institution appointed by the President, raising concerns about the supervisory function's independence. To address this, legal reforms are needed to create an independent supervisory institution with complete organizational autonomy, defining its structure, decision-making processes, and financial independence. This will prevent undue influence from external factors, such as political influence, and ensure a secure digital environment for all stakeholders.
Keywords**:** Protection of Personal Data Law; Independent Supervisory Institution.

1 Introduction

Information and Communications Technology (ICT) and digital transformation have fundamentally changed the balance of the world. Nowadays, the presence of technology makes it possible to trace the patterns of human behaviour. The advent of information technology has resulted in the dissolution of traditional boundaries and has had a profound impact on social change. This has led to the development of information technology becoming a double-edged sword, with the potential to enhance the welfare of society and the advancement of human civilisation. However, it can also be utilised as a means to facilitate illicit activities.[1] One of the most significant challenges associated with digital transformation is the issue of privacy. In reality, humans are now engaging in the sharing of information and data as a fundamental aspect of big data connectivity, including activities such as searching, collecting, investigating, and analyzing behavior. This has implications for

* Corresponding Author: nopriantobachtiar@gmail.com

the expansion of the scope of protection of privacy rights, which was originally limited to the real world, now also including the realm of cyberspace and electronics.[2]

In the digital era, the development of information and communication technology has brought about significant changes to people's lives. In the process, personal data has become increasingly important and sensitive, as many activities are conducted online. Personal data includes information such as name, address, identity number, financial information, medical history, and other sensitive information relating to individuals.[3] The vast majority of devices are now connected to the internet, allowing for remote management from any location. As people increasingly utilize digital technology in their daily lives to enhance work efficiency, foster socio-economic relationships, and facilitate other activities, the consequences of this period are considerable. The development of computer-based technology for information and communication has occurred at a rapid pace within society. These technological advancements subsequently facilitate the activities of individuals.[4]

The Government adopted Law No. 27 of 2022 on the Protection of Personal Data, which is projected as a legal instrument that can respond to the situation where there are no standards, criteria for the protection of personal data, and includes a mandate for the establishment of an authority that consistently applies the principles of personal data protection. The existence of a personal data protection authority or institution is very important to ensure the effectiveness of the implementation of Law No. 27 of 2022 on the Protection of Personal Data, which will be carried out on the basis of the principles, rules, procedures and objectives of the establishment of the authority, as well as to ensure the compliance of the public and private sectors with the principles and legal provisions of personal data protection. In addition, this authority will in the future be the spearhead of the policy implementers who will supervise and raise the awareness of private actors and public authorities in their efforts to protect personal data.

The management of personal data and information in Indonesia is regarded as a matter of great importance. It is crucial that these assets are protected by a robust security system to minimize the risk of data theft or breach. This is particularly important in Indonesia, where the impact of these crimes is felt most acutely through the misuse of personal data and information by those who lack responsibility and accountability. In addition to the necessity for supervision and assurance of effective and ethical data management, it is also necessary for there to be a regulation pertaining to cybercrime. The regulation must also address the protection of personal data and information in Indonesia.[5]

In essence, supervisory authorities represent the tangible embodiment of the principle of personal data protection. Its principal role encompasses the implementation of data protection and privacy policies, as well as the raising of awareness and the provision of consultation services, in addition to developing networks. These roles are outlined in Article 58 of the Law No. 27 of 2022 on the Protection of Personal Data. In accordance with the stipulations of Law No. 27 of 2022 on the Protection of Personal Data, the implementation of the supervisory function of personal data protection is entrusted to an institution appointed by and responsible to the President. The specifics of its duties and authorities are further delineated in a Presidential Regulation (Articles 59 and 60 of Law No. 27 of 2022 on the Protection of Personal Data). In essence, this institution will perform three primary functions: legislative and regulatory, supervisory, and administrative-executive. In addition, it will possess the powers of dispute resolution and adjudication in accordance with the duties and authorities entrusted to it.

The discussion on the supervisory authority of personal data protection is of significant importance, particularly in the context of Indonesia, which currently lacks a dedicated institution responsible for overseeing the protection of personal data. To date, the supervisory authority responsible for the supervision of personal data protection has been an institution appointed and answerable to the President. The details of its duties and authorities are further

regulated in the Presidential Regulation, which has not been operating effectively. The issue of data privacy has received considerable attention in Indonesia, reflecting concerns about the increasing incidence of data breaches and misuse in the context of the country's transition to digital technologies. However, this transition has not been accompanied by the implementation of comprehensive legal protections.

Therefore, this article explores the following research questions: What is the urgency of establishing an independent supervisory institution in law enforcement for the protection of personal data in Indonesia? How can the legal reform of the establishment of an independent supervisory institution for the enforcement of personal data protection law in Indonesia?

2 Method

This type of research uses normative juridical research methods, using a statutory approach and an analytical approach.[6] The primary legal material is Law No. 27 of 2022 on the Protection of Personal Data, followed by analysis through grammatical interpretation and teleological interpretation.[7]

3 Discussion and Analysis

3.1 The Urgency of Establishing an Independent Supervisory Institution in Law Enforcement for The Protection of Personal Data in Indonesia

The term "personal data" refers to information that is owned and protected by an individual, and which cannot be publicly disclosed without consent. This information is related to the right to privacy. In several international and regional instruments, including the European Union Data Protection Directive, the European Union Data Protection Convention, and the OECD Guidelines, the term "personal data" is defined as any data that can be linked to a specific or identifiable individual.[8] In a more general sense, personal data can be defined as information pertaining to an individual. This data often contains information that is considered so personal by the person in question that he or she desires to keep it private and restrict access. In a more explicit sense, personal data can be defined as information that is closely related to a person and is used to distinguish characteristics for each individual.[9]

The protection of personal data is of paramount importance in the context of the development of cybersecurity and the enhancement of national sovereignty capabilities. These capabilities, which are owned by a country, including Indonesia, are essential for the protection of citizens' data. The fundamental principle is the entitlement of each citizen to possess the capacity to safeguard their data and to receive assurance of protection from the state, thereby ensuring their security and freedom in cyberspace.[10] The field of personal data protection is distinguished by a differentiation between general and sensitive personal data. This differentiation is based on the extent to which the disclosure of the data would cause harm to the data owner if the data were processed without consent. The term "sensitive" data is typically associated with greater legal protection.[11] Legal protection is to provide protection to human rights that are harmed by others and this protection is given to the community so that they can enjoy all the rights granted by law.[12]

The right to privacy and protection of personal data have been universally recognized as fundamental human rights and guaranteed by the Constitution of the Republic of Indonesia through Article 28, paragraph (1) of the 1945 Constitution, which also implicitly states the constitutional responsibility and obligation of the state to safeguard citizens' privacy rights through the protection of personal data. The enactment of the Law No. 27 of 2022 on the Protection of Personal Data as a comprehensive legal framework has indeed provided a basis

and legal certainty for protecting citizens' rights related to personal data. Nevertheless, the effectiveness of the Law No. 27 of 2022 on the Protection of Personal Data is contingent upon the existence of an independent regulatory body that can act as a supervisor for the enforcement of privacy and personal data laws.

In response to concerns about the protection of personal data at the national level, the House of Representatives passed the Law No. 27 of 2022 on the Protection of Personal Data on 20 September 2022. This was prompted by international scrutiny of personal data protection regulations, resulting in the enactment of special legal instruments such as the PDP Law in 132 countries. At the ASEAN level, Indonesia is the fifth country to have passed a personal data protection law, following Malaysia, Singapore, the Philippines and Thailand. Upon examination of the substance of the Law No. 27 of 2022 on the Protection of Personal Data, it becomes evident that it regulates a number of crucial matters. Article 4 lists the categories of personal data, which are defined as follows: "Personal Data consists of: a. Specific personal data; and b. General personal data." Furthermore, Article 5 to Article 15 affirm the rights of data subjects. This set of articles discusses the rights that individuals have attached to their personal data. In addition to the aforementioned rights, the legislation also encompasses the obligations of data controllers. These are defined as any person, public body or international organization that acts independently or in conjunction with others to achieve the purposes set out in the law and to regulate the processing of personal data. The specific obligations of data controllers are set out in Articles 20 to 50. Furthermore, the law states that the establishment of a personal data protection institution shall be under the direct authority of the President, as set out in Article 58 to Article 60.[13]

The process of law enforcement is the means by which legal desires are brought into fruition. The desire of the law is nothing but the thoughts of the law-making body, which have been formulated into rules of law. The rule of law is a formulation of the thoughts of lawmakers, and as such, it also determines the ways in which law enforcement is carried out.[14] The protection of personal data is of paramount importance in the context of the digital age. Law enforcement plays a pivotal role in this regard. The protection of individuals' privacy rights is not the sole objective of data protection legislation; it also serves to ensure that personal data is not misused or illegally accessed in an increasingly digitally connected environment. The enactment of robust legislation and the implementation of rigorous enforcement mechanisms are pivotal to ensuring that personal data is managed in accordance with established legal standards. Furthermore, effective enforcement contributes to the public's trust in digital services and businesses, as it provides assurance that violations of personal data protection policies will be taken seriously.

Indonesia currently has comprehensive data protection legislation that is comparable to that of developed countries. However, the effectiveness of these laws and regulations has yet to show significant signs of improvement. There is a high incidence of data leaks involving Indonesian citizens, and there is a lack of coordination between authorized ministries and agencies, which has resulted in ongoing problems. The establishment of an independent oversight institution in the field of personal data protection oversight would be beneficial in effectively enforcing existing laws and regulations. This will significantly enhance the protection of personal data from misuse, breach and unauthorized access, thereby safeguarding the privacy rights of individuals across the country. The issue of personal data leakage represents a significant and pervasive concern that can result in significant adverse effects, including financial losses, the creation of false identities, and the further exploitation of data. In light of the aforementioned issues, it is imperative that both governments and private entities raise public consciousness regarding data security. Furthermore, it is crucial that they adopt appropriate preventative measures to safeguard personal data. It is of the utmost importance to remain informed about the latest developments in data security issues in Indonesia or any other country.[3]

In light of the authorities and duties assigned to the Independent Supervisory Institution concerning policy-making, supervision, and law enforcement, as outlined in Articles 59 and 60 of the Law No. 27 of 2022 on the Protection of Personal Data, it is imperative to establish a specific state institution with autonomous characteristics. In terms of institutional status, the Independent Supervisory Institution is no longer a truly independent regulatory authority, as its formal independence is not mandated by law but rather by Presidential Regulation. However, within the classification of supporting state institutions, there are recognized independent agencies that are intended to function as government bodies within the executive realm, distinct from executive agencies or ministries/departments. Furthermore, given the comprehensive nature of data protection regulations in Indonesia, which extend to both the public and private sectors, it is of the utmost importance that the implementing body be independent in order to ensure the effectiveness and objectivity of its operations.[15]

Although the Law No. 27 of 2022 on the Protection of Personal Data has established a personal data protection implementing institution under the executive branch (the President), this institution must be independent in carrying out its functions, duties, and authorities and free from influence and intervention from any party. This is of significant importance, as the implementation of the authority's function in personal data protection encompasses not only individuals and private entities, but also public bodies (government). Consequently, institutional independence, personal independence, and independence in exercising functions/authorities are essential, free from both personal and political influence. The independence of the supervisory institution is designed to ensure that its decisions, functions, duties, and authorities are not influenced by external factors, including intervention, the interests of individuals, politics, or any other institution. This independence is guaranteed by the Law No. 27 of 2022 on the Protection of Personal Data and its implementing regulations, which stipulate that the institution must be free from the political will of the President as the highest executive authority.

The term "independent state institution" is the one most commonly used by constitutional law experts and scholars, despite the fact that some argue that the term "state auxiliary institution" or "independent state institution" is preferable. M. Laica Marzuki again avoids confusion with other institutions that sit below constitutional state institutions by using the term "state auxiliary institutions" instead of "independent state institutions." This is done to avoid confusion with other institutions that sit below constitutional state institutions. These institutions are not in the executive, legislative, or judicial branches of power.[16] Nonetheless, they cannot be considered private organizations or non-governmental organizations despite certain parallels with these entities, as their funding is derived from public sources, and their purpose is to serve the public interest. Consequently, they are more accurately classified as non-governmental organizations.[17]

The importance of law enforcement without interference or intervention from individuals, politics, or any institution in making decisions, executing functions, duties, and authorities as stipulated in the Law No. 27 of 2022 on the Protection of Personal Data and its implementing regulations, including freedom from the political will of the President as the highest executive authority in the context of personal data protection lies in ensuring impartiality, integrity, and effectiveness of the legal framework. This ensures that the protection of personal data is carried out objectively and in accordance with established laws, safeguarding individuals' rights to privacy and data protection without undue influence or bias. It promotes trust in regulatory bodies and enhances compliance with data protection standards, ultimately contributing to a secure digital environment for all stakeholders.

Furthermore, the establishment of a robust data protection framework is crucial to enhance trust and stimulate innovation within Indonesia's sustainable development in the digital era. The establishment of independent institutions will provide clear guidance and oversight, thereby creating a safe and reliable environment for businesses and individuals

alike. This environment will foster innovation, attract foreign investment, and support sustainable development by ensuring that data handling practices are transparent and accountable.

3.2 The Legal Reform of The Establishment of an Independent Supervisory Institution for The Enforcement of Personal Data Protection Law in Indonesia

Law as a tool of social engineering must be used to provide a way for various developments that occur in society, especially developments in the field of information technology that are increasingly rapid with the times. The advent of a new legal regime has brought about the regulation of information technology, which is now referred to as "cyber law." The term cyber law is more appropriate for this research, as the word "cyber" has been identified with cyberspace and is sufficient to address issues related to proof and law enforcement. Law enforcement may encounter difficulties if they have to prove a problem that is assumed by the term "cyberspace," which is an invisible and pseudo-form.[1] In the context of the regulation and protection of personal information in the digital era, the relationship between cyber law and personal data protection legislation is one of close interconnection.

Cyber law encompasses the regulations that govern the utilization of digital technology, as well as cybersecurity, which represents a significant aspect of personal data protection. These regulations impose constraints on the collection, utilization, retention and dissemination of personal data by both public and private entities. In this context, law enforcement encompasses the investigation of offences, such as illegal access, identity theft, or data leakage, utilizing digital evidence and forensic analysis to prosecute cyber criminals. Furthermore, cyber law facilitates international cooperation in the enforcement of personal data protection laws, including in terms of extradition, information exchange, and harmonization of cross-border regulations. In light of the rapid development of technology, cyber law also enables regulatory updates to address new challenges, such as AI, IoT, and big data, which increasingly affect the management and security of personal data. The cyber law framework not only regulates the use of digital technologies in general, but provides a solid foundation for the safeguarding of security, privacy, and individual rights in the ever-evolving digital age.

It is becoming increasingly common for countries to recognize data protection as either a constitutional right or in the form of data habeas. Data habeas, also known as the right to data protection, allows individuals to have their data secured and to be able to justify it when errors are found. In this context, it is evident that the right to personal data protection is not merely of importance but also a fundamental aspect of the individual's dignity and freedom. The implementation of robust data protection measures can serve as a significant catalyst for the advancement of political, spiritual, and religious freedom.[18] The protection of privacy rights and individual personal data has become a constitutional obligation of the state, as set out in Article 28G, paragraph (1), of the 1945 Constitution of the Republic of Indonesia. This protection is inextricably linked to the existence of legislation as a means of safeguarding the constitutional rights of all individuals. Furthermore, the existence of personal data represents a manifestation of the existence of strategic assets with high economic value, thus potentially leading to instances of misuse of personal data that have the potential to violate the integrity of privacy.[13]

In the event that the law in question is perceived to be inappropriate or inadequate for use in community life, the community will seek a change in the law. This will result in legal reform to free victims from the deficiencies in the law. Legal reform is initiated by the bodies of law-forming power, which include the judiciary and law-making institutions such as the government and authorized legislative bodies, taking the necessary steps to ensure the

enforcement of existing laws and regulations. The objective of legal reform is to ensure that the legal rules and principles contained within these laws and regulations can adequately fulfil their respective objectives and serve as a system of laws for a country.[19] The term 'legal reform' refers to a process by which various formulations of legal provisions and legislation are subjected to examination in order to identify potential areas for improvement. The aim is to implement changes that enhance efficiency, promote justice and facilitate the application of applicable law.[20]

One crucial factor to be considered is that any activities or sites visited via internet-connected devices will be meticulously recorded, forming a comprehensive digital footprint which may potentially be exploited to facilitate illegal activities. This therefore becomes a sensitive and complex discourse, one which concerns the misuse of personal data protection against third parties. In light of these concerns, various countries and international institutions have sought to address this issue through the implementation of legal frameworks related to personal data processing.[18] In Indonesia, there is currently a significant number of legal issues pertaining to the leakage and misuse of personal data for personal gain.[21] One of the defining characteristics of the digital era is the challenge it presents to the privacy of personal data. The nature of digitized information, which encourages an environment that does not respect the privacy of personal data, is a significant factor in this regard. Personal data is easily collected and shared, which in turn creates an environment that does not respect the privacy of personal data.[22]

The Law No. 27 of 2022 on the Protection of Personal Data was enacted with the objective of safeguarding individuals' personal data and ensuring legal certainty in the event of data misuse, including data leaks, which are prevalent in Indonesia. The implementation of Law Number 27 Year 2022 on Personal Data Protection will undoubtedly be facilitated by the existence of derivative regulations or implementing regulations in the form of Government Regulations. This is because the Law No. 27 of 2022 on the Protection of Personal Data in Indonesia has not yet provided a detailed framework for the implementation of personal data protection, which will be developed by an independent institution authorized and appointed by the President in the future.[23]

The oversight of personal data protection is currently assigned to an institution appointed by and accountable to the President. This setup raises concerns about the independence of the supervisory function. The specific responsibilities and authorities of this institution are detailed in a Presidential Regulation, as outlined in Articles 59 and 60 of the law. This configuration demonstrates a deficiency in the autonomy of the supervisory function, which may compromise its ability to enforce personal data protection laws in an impartial manner. To address this concern, it is imperative to implement legal reforms to create an independent supervisory institution with the sole responsibility of enforcing personal data protection laws in Indonesia. Initially, legislative amendments should be enacted to mandate the establishment of this independent institution with complete organizational autonomy. This encompasses defining its structure, decision-making processes, and financial independence in order to ensure that it is not influenced or interfered with by external factors such as direct political influence.

Furthermore, it is of the utmost importance to separate the institution in question from the direct control of the executive branch. This is a crucial step in enhancing the institution's independence. This can be accomplished by placing the entity under a distinct branch of government, such as the judiciary, or by establishing the entity as a novel independent body that reports to the legislature. Such a separation of powers would serve to mitigate conflicts of interest and to bolster confidence in the impartial enforcement of data protection regulations. In addition, any reforms should include a transparent set of criteria and procedures for the appointment of the institution's leadership. The selection of leaders should

be conducted through a process that is based on merit and ensures expertise in data protection, as well as independence from political affiliations.

The implementation of fixed terms of office and protections against arbitrary dismissal would serve to further fortify the institution's independence, as well as guarantee its continuity of oversight. It is similarly crucial to grant the independent supervisory body operational autonomy. This encompasses autonomy in budget management, staffing decisions, and the authority to issue enforceable decisions and penalties independently of external influences. It is thus recommended that these mechanisms include the obligation to provide regular reports to the public, the holding of public hearings, and oversight by the legislature. These measures will ensure the continued accountability of the institution to the public.

3.3 Comparative Analysis of the Implementation of Independent Data Privacy Institutions in Various Countries

In the era of digital transformation, personal data protection has become a key concern worldwide. The establishment of independent supervisory institutions to oversee data privacy regulations is crucial for safeguarding personal information from misuse and ensuring compliance with legal standards. While many countries have enacted comprehensive data protection laws, the effectiveness of these laws often hinges on the autonomy and capabilities of the institutions tasked with their enforcement. This article explores the implementation of independent data privacy institutions in various countries, examining their structures, operational mechanisms, and effectiveness in enforcing data protection laws. By analyzing examples from different legal frameworks, this article aims to provide insights that can inform legal reforms in countries such as Indonesia, which is in the process of strengthening its personal data protection framework.

3.3.1 European Union: General Data Protection Regulation (GDPR) and Independent Supervisory Authorities

The European Union’s General Data Protection Regulation (GDPR) is one of the most comprehensive data protection frameworks in the world. A key feature of the GDPR is the establishment of independent supervisory authorities (SAs) in each member state.[24] These authorities are responsible for monitoring compliance with GDPR, handling complaints, conducting investigations, and imposing penalties. The independence of these authorities is crucial, as it ensures that they can act without undue influence from the government or private entities.

For example, Germany’s Federal Commissioner for Data Protection and Freedom of Information (BfDI) is one of the most prominent data protection authorities in the EU. It operates independently, has its own budget, and has the authority to impose significant fines for non-compliance. The BfDI’s independence from political influence is a key factor in its effectiveness in enforcing GDPR regulations. Similarly, France’s Commission Nationale de l'Informatique et des Libertés (CNIL) plays a pivotal role in ensuring that data protection laws are adhered to, particularly in cases involving large multinational corporations. CNIL's autonomy allows it to conduct thorough investigations and enforce data protection laws impartially.

3.3.2 United States: Federal Trade Commission (FTC) and Sectoral Approach to Data Privacy

The United States has taken a sectoral approach to data privacy, where different industries are regulated by different laws. While the U.S. does not have a single, comprehensive data protection law like the GDPR, the Federal Trade Commission (FTC) plays a significant role in overseeing data privacy issues. The FTC is an independent agency, and its main focus is on consumer protection, including protecting consumer data from deceptive and unfair practices.[25]

The FTC's authority to regulate data privacy is somewhat limited compared to European supervisory authorities, as it often relies on other laws, such as the Federal Trade Commission Act, to enforce data protection. However, it has been effective in holding companies accountable for data breaches and privacy violations through enforcement actions and consent decrees. The sectoral nature of U.S. data privacy laws means that the FTC must work closely with other agencies, such as the Department of Health and Human Services (for healthcare data under HIPAA), to ensure compliance in specific industries.

3.3.3 Singapore: Personal Data Protection Commission (PDPC)

Singapore's Personal Data Protection Act (PDPA) is a comprehensive legal framework that governs the collection, use, and disclosure of personal data by private organizations. The Personal Data Protection Commission (PDPC) is the independent regulatory body responsible for administering and enforcing the PDPA. The PDPC has wide-ranging powers, including the ability to investigate complaints, conduct audits, and impose financial penalties on organizations that fail to comply with the PDPA.[26]

One of the strengths of the PDPC is its focus on public awareness and education. It actively engages with businesses and the public to promote understanding of data protection principles. The PDPC's independence from government and private sector influence ensures that it can enforce the law impartially and effectively. Additionally, Singapore's small size and centralized government structure allow the PDPC to implement data protection measures quickly and efficiently.

3.3.4 South Korea: Personal Information Protection Commission (PIPC)

South Korea's Personal Information Protection Commission (PIPC) is an independent regulatory body that oversees the enforcement of the Personal Information Protection Act (PIPA), one of the strictest data protection laws in Asia. The PIPC is tasked with investigating data breaches, issuing sanctions, and ensuring that both public and private organizations comply with PIPA.[24]

The independence of the PIPC is enshrined in law, and it has the authority to conduct investigations and impose penalties without interference from other branches of government. South Korea's legal framework for data protection has been recognized for its robustness, particularly in light of the country's highly digitalized economy. The PIPC's success in enforcing data protection laws can be attributed to its financial and operational independence, as well as its ability to adapt to the evolving challenges of the digital age.

3.3.5 Brazil: National Data Protection Authority (ANPD)

Brazil's General Data Protection Law (LGPD) closely mirrors the GDPR in its approach to data protection, and the National Data Protection Authority (ANPD) is the body responsible for enforcing it. The ANPD was established as an independent agency, although it initially operated under the executive branch of the government. Over time, there has been increasing advocacy for strengthening the ANPD's autonomy to ensure that it can enforce the LGPD without political interference.[24]

The ANPD is responsible for ensuring that public and private entities comply with data protection regulations, handling complaints, and conducting investigations. While the ANPD is still in its early stages, its development as a fully independent body is critical for ensuring the long-term effectiveness of Brazil's data protection framework.

The examples of independent data privacy institutions from the European Union, United States, Singapore, South Korea, and Brazil demonstrate that autonomy and independence are critical for effective enforcement of data protection laws. These institutions must be free from political or external influence to function impartially and uphold the integrity of data privacy regulations. Indonesia, which is in the process of reforming its data protection framework, can draw valuable lessons from these countries. By establishing a fully independent supervisory institution, Indonesia can strengthen its legal framework for personal data protection and enhance public trust in its digital economy.

4 Conclusion

The importance of law enforcement without interference or intervention from individuals, politics, or any institution in making decisions, executing functions, duties, and authorities as stipulated in the Law No. 27 of 2022 on the Protection of Personal Data and its implementing regulations, including freedom from the political will of the President as the highest executive authority in the context of personal data protection lies in ensuring impartiality, integrity, and effectiveness of the legal framework. This ensures that the protection of personal data is carried out objectively and in accordance with established laws, safeguarding individuals' rights to privacy and data protection without undue influence or bias. It promotes trust in regulatory bodies and enhances compliance with data protection standards, ultimately contributing to a secure digital environment for all stakeholders.

In Indonesia, the responsibility for overseeing the protection of personal data currently lies with an institution that has been appointed by and is accountable to the President. This configuration raises concerns about the independence of the supervisory function. The specific responsibilities and authorities of this institution are delineated in a Presidential Regulation, as outlined in Articles 59 and 60 of the law. Such a framework indicates a lack of autonomy for the supervisory function, which may hinder its capacity to enforce personal data protection laws impartially. To address this concern, it is imperative to implement legal reforms to create an independent supervisory institution with the sole responsibility of enforcing personal data protection laws in Indonesia. In the initial stages, the legislature must enact amendments to mandate the establishment of this independent institution with complete organizational autonomy. To this end, it is necessary to define its structure, decision-making processes and financial independence in order to prevent any undue influence or interference from external factors, such as direct political influence.

To enhance the protection of personal data in Indonesia, it is crucial to establish a truly independent supervisory institution, free from executive control to ensure impartial and effective enforcement of Law No. 27 of 2022 on Personal Data Protection. This institution should possess complete operational autonomy, including independent management of its budget, staffing, and decision-making processes, allowing it to issue binding decisions and

impose penalties without external interference. The leadership of the institution must be selected through a transparent, merit-based process that prioritizes expertise in data protection and guarantees independence from political influence. Fixed terms of office and protections against arbitrary dismissal should be implemented to further safeguard the institution's integrity. Additionally, the supervisory body must be held accountable to the public through regular reporting, public hearings, and legislative oversight. This will ensure transparency, maintain public trust, and strengthen the institution's ability to enforce data protection laws across both public and private sectors, fostering a secure digital environment conducive to innovation and economic growth in Indonesia.

References

[1] A. M. Ramli, *Cyber Law & HAKI*. Bandung: Refika Aditama, 2006.
[2] D. Budhijanto, *Cyber Lawdan Revolusi Industri 4.0*. Bandung: Logoz Publishing, 2019.
[3] K. R. A. Suari and I. M. Sarjana, "Menjaga Privasi Di Era Digital: Perlindungan Data Pribadi Di Indonesia," *J. Anal. Huk.*, vol. 6, no. 1, pp. 132–142, 2023, doi: https://doi.org/10.38043/jah.v6i1.4484.
[4] C. Hadita, "Registrasi Data Pribadi Melalui Kartu Prabayar Dalam Perspektif Hak Asasi Manusia," *J. HAM*, vol. 9, pp. 191–204, 2018, doi: https://doi.org/10.30641/ham.2018.9.191-204.
[5] R. Aswandi, "Perlindungan Data Dan Informasi Pribadi Melalui Indonesian Data Protection System (IDPS)," *Legis. (Lembaran Gagasan Mhs. Yang Solut. Dan Inov.*, vol. 3, no. 2, pp. 167–190, 2020.
[6] P. M. Marzuki, *Penelitian Hukum: Edisi Revisi*. Jakarta: Kencana, 2019.
[7] S. Mertokusumo, *Mengenal Hukum Suatu Pengantar*. Yogyakarta: Universitas Atma Jaya Yogyakarta, 2010.
[8] U. Mutiara and R. Maulana, "Perlindungan Data Pribadi Sebagai Bagian Dari Hak Asasi Manusia Atas Perlindungan Diri Pribadi," *Indones. J. Law Policy Stud.*, vol. 1, p. 50, 2020, doi: http://dx.doi.org/10.31000/ijlp.v1i1.2648.g1629.
[9] S. D. Rosadi, *Cyber Law: Aspek Data Privasi Menurut Hukum Internasional, Regional Dan Nasiona*. Bandung: Refika Aditama, 2015.
[10] M. P. Aji, "Sistem Keamanan Siber Dan Kedaulatan Data Di Indonesia Dalam Perspektif Ekonomi Politik (Studi Kasus Perlindungan Data Pribadi) [Cyber Security System and Data Sovereignty in Indonesia in Political Economic Perspective]," *J. Polit. Din. Masal. Polit. Dalam Negeri Dan Hub. Int.*, vol. 13, no. 2, pp. 222–238, 2023, doi: https://doi.org/10.22212/jp.v13i2.3299.
[11] S. Rosadi, "Konsep Perlindungan Hukum Atas Privasi Dan Data Pribadi Dikaitkan Dengan Penggunaan Cloud Computing Di Indonesia," *Yust. J. Huk.*, vol. 1, p. 414, 2016, doi: https://doi.org/10.20961/yustisia.v0i94.2780.
[12] S. Rahardjo, *Ilmu Hukum*. Bandung: Citra Aditya Bakti, 2012.
[13] M. Fikri and S. Rusdiana, "Ruang Lingkup Perlindungan Data Pribadi: Kajian Hukum Posistif Indonesia," *Ganesha Law Rev.*, vol. 5, no. 1, 2023, [Online]. Available: https://ejournal2.undiksha.ac.id/index.php/GLR/article/view/2237.
[14] S. Rahardjo, *Penegakan Hukum Sebagai Tinjauan Sosiologis*. Yogyakarta: Genta Publishing, 2009.
[15] A. F. Faizah, "Penguatan Pelindungan Data Pribadi Melalui Otoritas Pengawas Di Indonesia Berdasarkan Perbandingan Hukum Hong Kong Dan Singapura," *Hakim J. Ilmu Huk. Dan Sos.*, vol. 1, no. 3, 2023, doi: https://doi.org/10.51903/hakim.v1i3.1222.
[16] R. Ramadani, "Lembaga Negara Independen Di Indonesia Dalam Perspektif Konsep

Independent Regulatory Agencies," *J. Huk. Ius Quia Iustum*, vol. 27, no. 1, pp. 169–92, 2020.

[17] A. Mahardika, "Desain Ideal Pembentukan Otoritas Independen Perlindungan Data Pribadi Dalam Sistem Ketatanegaraan Indonesia," *J. Huk. Unissula*, vol. 37, no. 2, pp. 101–118, 2021, doi: https://doi.org/10.26532/jh.v37i2.16994.

[18] E. Fauzy and N. A. R. Shandy, "Hak Atas Privasi Dan Politik Hukum Undang-Undang Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi," *Lex Renaiss.*, vol. 7, no. 3, pp. 445–461, 2023, doi: https://doi.org/10.20885/JLR.vol7.iss3.art1.

[19] A. Rifai, *Penemuan Hukum Oleh Hakim Dalam Perspektif Hukum Progresif*. Jakarta: Sinar Grafika, 2010.

[20] T. Prasetyo, *Pembaharuan Hukum Perspektif Teori Keadilan Bermartabat*. Malang: Setara Press, 2017.

[21] M. Rifqy, H. Arham, and M. C. Risal, "Perlindungan Data Pribadi Bagi Pengguna Media Sosial," *J. Al Tasyri'iyyah*, vol. 3, p. 110, 2023, doi: https://doi.org/10.24252/jat.vi.44108.

[22] F. Rahman, "Kerangka Hukum Perlindungan Data Pribadi Dalam Penerapan Sistem Pemerintahan Berbasis Elektronik Di Indonesia," *J. Legis. Indones.*, vol. 18, no. 1, pp. 81–102, 2021, doi: https://doi.org/10.54629/jli.v18i1.736.

[23] C. Vania, "Tinjauan Yuridis Terhadap Perlindungan Data Pribadi Dari Aspek Pengamanan Data Dan Keamanan Siber," *J. Multidisiplin Indones.*, vol. 2, no. 3, pp. 654–666, 2023, doi: https://doi.org/10.58344/jmi.v2i3.157.

[24] H. P. Rudo, "The global landscape of data privacy: Important points about new laws in three key jurisdictions," DLA Piper.

[25] J. G. Henderson, "FTC Releases 2023 Privacy and Data Security Update," Federal Trade Commission.

[26] Anonymous, "Comparing Privacy Laws: GDPR v. PIPL," Data Guidance.