Journal of General Education and Humanities
Vol. 5, No. 2, April 2026, pp. 2667 – 2675, https://doi.org/10.58421/gehu.v5i2.1252
ISSN 2963-7147

Analysis of Institutional Duties Regulations in Article 58 of Law Number 27 of 2022 concerning Personal Data Protection

Enis Tristiana
Universitas Sebelas Maret, Indonesia, Indonesia

Article Info

Article history:

Accepted 2026-03-03
Revision 2026-03-16
Accepted 2026-04-11

Keywords:

Data Integration
Personal Data Controller
Supervisory Authority

ABSTRACT

The protection of personal data is part of human rights, including the protection of individual privacy, as guaranteed in the Constitution of the Republic of Indonesia of 1945. The development of information technology encourages an increase in the collection and processing of personal data by state institutions and corporations, so that it has the potential to cause data misuse. Therefore, a clear legal basis is needed to ensure the security and protection of citizens' personal data. Law Number 27 of 2022 concerning Personal Data Protection is present as a legal basis in providing legal certainty and protection for data owners. This research aims to analyze the personal data protection arrangements and the role of institutions regulated in Article 58. The method used is normative legal research with a legislative and conceptual approach. The results of the study show that, even though the legal basis is available, the regulation of supervisory institutions' duties and authority still needs clarification. The implication is that institutional strengthening is needed to ensure effective supervision and protection of personal data.

Corresponding authors:

Enis Tristiana
Universitas Sebelas Maret, Indonesia
Email: enistristiana@staff.uns.ac.id

1. INTRODUCTION

The right to protection for all citizens, as stated in the 1945 Constitution of the Republic of Indonesia, is a constitutional right. This results in the state having the main obligation to guarantee and protect these rights as a constitutional responsibility in accordance with the provisions contained in Article 28G paragraph (1) of the 1945 Constitution of the Republic of Indonesia, namely "Everyone has the right to the protection of personal self, family, honor, dignity, and property under his power, as well as the right to a sense of security and protection from the threat of fear to do or not do something that is the Basic which is true." All residents of the country have a right to privacy that cannot be taken away or used by anyone without pressure [1], [2], [3].

The increase in cases in recent years reflects the growing concern about personal data breaches in Indonesia. In the 2019-2022 period, the Ministry of Communication and Information Technology has handled 77 data breach cases. Of those, 58 cases have been resolved while 19 are still in process, Johnny G. Plate said. The theft of personal data is not limited to individual citizens; it also involves private companies, government agencies, and even the country itself. So, personal data leakage is not a problem that can be ignored. The government's top priority should be protecting personal data to safeguard its citizens [4].

The Indonesian people saw a new opportunity when the Personal Data Protection Law No. 27 of 2022 was passed on October 17, 2022. Prior to this, the country had no regulations or enforcement mechanisms to oversee the protection of personal information. This regulation is intended to provide an efficient legal basis for protecting personal data while recognizing and respecting its importance. This issue became inefficient in previous legislation regarding the protection of personal data. Previously, the constitution had stipulated provisions related to this matter. While several previous laws and regulations have addressed the issue of personal data, there has been no detailed explanation of how such data protection is implemented. These regulations include the following: [5] Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Electronic Transaction Information (UU ITE), Regulation of the Minister of Communication and Information Technology Number 20 of 2016 concerning the Protection of Personal Data in Electronic Systems, and Government Regulation Number 71 of 2019 concerning the Implementation of Electronic Systems and Transactions (PP PSTE).

The state must supervise the implementation of personal data protection through a supervisory institution (Supervisory Authority). The state's supervision of personal data protection is a manifestation of the realization of equality (balance) between users as data subjects and platforms as data controllers. These two entities must be aligned in digitizing activities such as e-commerce, e-education, electronic health (e-Health), and government administrative services (e-Government).7 Indonesia, through Presidential Regulation Number 82 of 2023 concerning the Acceleration of Digital Transformation and National Digital Service Integration, connects all digital services and formulates strategic steps among institutions (K/L) to unite them with the Public Company of the Printing Money of the Republic of Indonesia (PERURI), which serves as the leading sector.

The protection of personal data is part of human rights, including the protection of individual privacy, as guaranteed in the Constitution of the Republic of Indonesia of 1945. The development of information technology encourages an increase in the collection and processing of personal data by state institutions and corporations, so that it has the potential to cause data misuse. Therefore, a clear legal basis is needed to ensure the security and protection of citizens' personal data. Law Number 27 of 2022 concerning Personal Data Protection is present as a legal basis in providing legal certainty and protection for data owners. This research aims to analyze the personal data protection arrangements and the role of institutions regulated in Article 58. The method used is normative legal research with a legislative and conceptual approach. The results of the study show that, even though the legal basis is available, the regulation of supervisory institutions' duties and authority still needs

clarification. The implication is that institutional strengthening is needed so that the supervision and protection of personal data can be carried out effectively.

The question of whether the supervisory authority based on Article 58 of Law Number 27 of 2022 concerning Personal Data Protection is sufficiently independent is an important issue in the implementation of personal data protection in Indonesia. Normatively, Article 58 establishes a supervisory institution tasked with overseeing the implementation of personal data protection. However, the degree of its independence is still a matter of debate, as the institution is under the President; structurally, it remains within the scope of executive power. This condition poses potential limitations in carrying out the supervisory function objectively, especially when supervision must also be carried out on government institutions.

In international practice, data protection supervisory authorities are generally established as independent bodies, free from government influence, in order to carry out supervisory, law enforcement, and dispute-resolution functions in a neutral manner. Therefore, although Article 58 provides a legal basis for the establishment of a supervisory body, its level of independence is still considered insufficient. This shows the need for further institutional strengthening and regulation so that supervisory authorities can carry out their duties effectively and free from intervention.

This digitalization requires the consent of each party to use the platform, on the one hand, and to the use of personal data, on the other. It is a goodwill, in a philosophical sense, related to the actions of human beings and, even in morality, to making a balanced decision (justice) in the face of unequal relationships. Immanuel Kant, as a morality that prioritizes human freedom, encourages free will when making decisions, even though good intentions as good intentions do not always benefit the action takers. In this Kantian ethics, the intention, or moral intention, is the most important, not the result of the action.

The platform, as a data controller, is equivalent an the user as the data subject. Although it has philosophical equivalence, it is axiologically different because the current factual relationship between the platform and the user is paralyzed, and the platform is very strong over the user, especially regarding personal data, which is subject to data collection. This is due to the realization of consent to the processing of personal data that is not in accordance with the basis of processing as stated in Article 20 paragraph (2), 21, and 22 of the PDP Law and the principles of personal data processing as stated in Article 16 paragraph (2) of the PDP Law. Article 20, paragraph (2), of the PDP Law mandates the legal basis for data processing, one of which is the subject's consent. The unification of the consent column for the use of the platform with the processing of personal data forces the data subject to consent to the processing of his or her personal data. An unequal relationship in the realization of consent is very difficult, or in other words, the user cannot fight, because, in principle, the unification of the consent column is based on a take-it-or-leave-it approach. So, like it or not, users have to accept choices they do not want. Only a very powerful third party can realign this inequality, namely the state.

The personal data protection institution is a representative of the state to ensure that the imbalance in the relationship between users and the platform is balanced, fair and the platform is not arbitrary in processing personal data from the data subject, in the event of a

violation, this personal data protection institution can provide administrative and judicial sanctions and can mediate the settlement of disputes outside the court between the parties in the implementation of personal data protection8. The ideal self-protection institution is in the form of a non-ministerial institution (LNS), but in fact, it is not. The current form of personal data protection institution is at least a Non-Governmental Organization (LPNK) and its existence is in the government (executive) and is responsible to the President's responsibility as stipulated in Article 58 of the PDP Law.

The personal data protection institution must be established after October 17, 2024, in an institutional form in accordance with Article 58. In today's world, there are Multi-Supervisory, Duo-Supervisory, and Single-Supervisory Authorities. The institutional form of the single supervisory authority is divided into 2, namely the Independent Supervisory Authority and the Primary Supervisory Authority. Of the two main institutional designs, the most likely choice is based on the duties and authorities in Articles 59 and 60, which are relatively broad and large. In contrast, the institutional posture is relatively small; Indonesia needs to choose the form of an institutional single supervisory authority, especially the main supervisory authority, because the institutional form of independent supervisory authority is no longer possible by laws and regulations as stipulated in Article 58 paragraphs (3) and (4) of the PDP Law. However, the possible institutional form is the main supervisory authority; however, the regulator must establish a personal data protection institution that is functionally independent and does not violate laws and regulations, nor contradict the role and authority as stated in Articles 59 and 60 of the PDP Law. Regulators should learn from regulatory authorities in several other countries that have established these institutions and draw on their success stories in personal data protection. This will enrich the thinking of regulators to formulate institutions that are in accordance with the global and Indonesian personal data protection needs that are in line with the limitations of the PDP Law.

2. METHODS

The research method used in this study is normative legal research, or doctrinal law research, namely library research or document study, because this research is conducted and aimed only at written regulations and other legal materials. Doctrinal research includes research in the form of dogma or positive legal doctrine. After the author collected legal sources, in this study used the Approach Statute, which is an approach that refers to all laws and regulations related to legal issues.

Primary legal materials (laws and regulations) are sources of law that have direct binding power because they emanate from the applicable laws and regulations. In legal research, primary legal materials serve as the primary basis for analyzing the norms, principles, and legal provisions that govern a problem. Primary legal material can be in the form of the constitution, laws, government regulations, presidential regulations, and other laws and regulations relevant to the object of research. In the context of personal data protection, primary legal materials include the 1945 Constitution of the Republic of Indonesia and Law Number 27 of 2022 concerning Personal Data Protection. Secondary legal material (journal articles and legal commentaries) is legal material that provides explanation, analysis, or interpretation of primary legal material. Secondary legal materials

serve to strengthen arguments and help understand the concept and application of a legal rule in practice. Secondary legal material can be in the form of scientific journal articles, legal textbooks, research results, expert opinions, as well as legal comments or analyses related to the research topic. In research on personal data protection, secondary legal materials are used to examine academics' and legal practitioners' views on the implementation, institutions, and challenges in the implementation of personal data protection.

3. RESULTS AND DISCUSSION

Personal data is an individual right protected by the constitution. The protection of personal data is not only about protecting an individual's data, but also about providing assurance that the individual's fundamental rights and freedoms regarding data are protected. The protection of personal data is intended to ensure that these rights and freedoms are not violated by other persons or institutions that do not have the right to do so in accordance with the provisions of laws and regulations. The concept of personal data protection emphasizes that everyone has the right to determine their own fate, including whether they will share data. If data sharing is carried out, he also has the right to determine the conditions that must be met in a community. This means that personal data is a right that the state must protect.

The protection of personal data has been mandated as in Article 28G paragraph (1) of the Constitution of the Republic of Indonesia 1945 states that everyone has the right to the protection of personal self, family, honor, dignity, and property under his or her power, as well as the right to a sense of security and protection from the threat of fear of doing or not doing something that is a human right. It is also stipulated in Article 28H paragraph (4) that everyone has the right to have personal property rights, and such ownership rights must not be arbitrarily taken over by anyone. Based on the provisions in Article 28G paragraph (1) and Article 28H paragraph (4) of the 1945 Constitution of the Republic of Indonesia, the state is obliged to provide protection efforts to a person, both protection of a person's soul and body, as well as what everyone has, including data.

The constitution has mandated provisions regarding the protection of personal data, and the regulation of personal data is also regulated in several laws and regulations, including the following:

1. Law Number 19 of 2016 concerning Amendments to Law Number

   Article 26 paragraph (1) of 2008 concerning Electronic Transaction Information (ITE Law) states that, unless otherwise specified by laws and regulations, the use of information through electronic media regarding a person's personal data must be carried out with the consent of the person concerned.
2. Government Regulation Number 71 of 2019 concerning the Implementation of Electronic Systems and Transactions (PP PSTE) Article 14 paragraph (1) letters c and e states that Electronic System Operators (PSE) are obliged to apply the principle of personal data protection in carrying out personal data processing, including personal data processing by guaranteeing the rights of personal data owners and personal data processing carried out by maintaining the security of personal data

from loss, misuse, access and unauthorized disclosure, as well as alteration or destruction of personal data.

3. Regulation of the Minister of Communication and Information Technology Number 20 of 2016 concerning the Protection of Personal Data in Electronic Systems, Article 8 states that in obtaining and collecting personal data, electronic system operators must respect the rights of the owner of the personal data. Respect is achieved through the provision of the option to disclose or keep personal data confidential.

According to data from the Director General of Informatics Applications (Dirjen Aptika) in 2022, as many as 105 million data points on the Indonesian people related to general elections came from the General Election Commission, including data in the form of NIK, Family Card, full name, place and date of birth, gender, and age. Then, in July 2023, his party received information about an immigration data leak involving the Director General of Immigration (Directorate General of Immigration), which resulted in the disclosure of the personal data of all passports issued by the Indonesian government. This information was released by a Bjorka hacker who claimed to have access to passport numbers, passport expiration dates, place and date of birth, gender, and date of issue. From this amount of data, there may be a child's specific or sensitive data, so the risk posed is greater. In all cases of personal data leakage, there has been no imposition of sanctions or any more serious follow-up on the perpetrators. Therefore, the Supervisory Institution in Indonesia needs to be established immediately by the President, with the authority to supervise data users who control personal data. This is because there have been several cases of personal data leakage year after year. The regulation on the establishment of this Supervisory Institution is mentioned in the Personal Data Protection Law, but the term limit for its establishment is not.

The arrangements of the Personal Data Protection Supervisory Institution under the PDP Law include:

1. The government plays a role in implementing Personal Data Protection in accordance with the provisions of this law.
2. The implementation of Personal Data Protection, as referred to in the paragraph, is carried out by the institution.
3. The institution as referred to in paragraph (2) is determined by the President.
4. The institution, as intended in paragraph (2), is responsible to the President.
5. Further provisions regarding the institution, as intended in paragraph (2), are set out in the Presidential Regulation.

Article 58 paragraphs (1) to (5) of the PDP Law stipulate the form of implementation of personal data protection carried out institutionally. In paragraph (1), it is stated that the Government (Executive) has an obligation to realize the protection of personal data. Then, in paragraph (2) and paragraph (3), it is stated that an institution appointed by the President carries out the implementation of personal data protection.1 In paragraph (4), the institution is responsible to the President in carrying out its duties [6].

This shows that Indonesia has made efforts to fulfill its promise in personal data protection. This promise aligns with the protection of personal data that is also in place in

other countries. At least, the regulations governing the authority and duties of this personal data protection institution have met the minimum international standards for the regulation of personal data protection institutions, especially in several Southeast Asian countries.

The draft on the form, duties, and authority of the Personal Data Protection Supervisory Agency suggests that this institution has a special position. According to Jimly Ashiddiqie, institutions like this are commonly referred to as additional organs of state or *auxiliary institutions.* This term is defined as a supportive and independent State Institution [7].

In carrying out their roles and duties, independent State institutions have a mixed nature, drawing on various branches of State power. For example, the institution may exercise several powers in executive, legislative, and judicial functions. The authority carried by this institution is outside the norms for the duties and functions of State Institutions in general, as it has mixed functions and duties.

There are differences in the form of the Personal Data Protection Supervisory Institution regulated in the PDP Law. This institution can be classified as an Independent State Institution in terms of its roles and duties, yet it states that the President establishes it. Therefore, this institution is directly responsible to the President, which means that it does not have the nature of an Independent State Institution as a whole.

In the regulation of the PDP Law, there is no mention of the term limit of the President's term for the establishment of the Personal Data Supervisory Agency, this needs to be reviewed so that the period of establishment of the Supervisory Institution can be determined so that the function of imposing administrative sanctions can be imposed on perpetrators who violate the Personal Data Protection Law [8].

Institutional Independence Analysis

The regulation of supervisory institutions in Article 58 of Law Number 27 of 2022 concerning Personal Data Protection shows that the President established the institution and is responsible to the President. This provision has implications for the supervisory institution's level of independence, as it falls within the scope of executive power. In the practice of personal data protection supervision, independence is an important aspect, enabling supervisory institutions to carry out their functions objectively and free from political intervention or institutional interests. If the supervisory institution is under executive control, there is a potential conflict of interest, especially when it must supervise government institutions that are also part of the executive branch. This condition can affect the effectiveness of law enforcement and supervision of personal data protection violations [9].

Comparative Analysis

Compared with other countries, the institutional design of data protection supervisors shows a different level of independence. In the European Union, data protection supervisory authorities are established independently in accordance with the principles set out in the General Data Protection Regulation (GDPR). The authority has broad powers to supervise, investigate, and impose administrative sanctions for personal data protection violations,

without being under the direct control of the government. In Singapore, personal data protection is overseen by the Personal Data Protection Commission (PDPC), which is part of the government structure but still has special powers to supervise and enforce the law against personal data breaches. Meanwhile, in Malaysia, there is a Personal Data Protection Department led by the Commissioner for Personal Data Protection under the Ministry of Communications and Digital, which has the function of supervising and regulating the management of personal data by the private sector. This comparison shows that the level of independence of supervisory agencies in different countries may differ, but in general, it still emphasizes the importance of clear authority and effective oversight mechanisms [10].

Institutional Design Model

In international practice, there are several models of institutional design in the supervision of personal data protection. The first model is an independent supervisory authority, an institution that stands independently and is not under a specific branch of power. This model is widely applied across many European countries because it is considered capable of guaranteeing objectivity, accountability, and the effectiveness of supervision in addressing personal data protection breaches. The second model is an executive-based supervisory authority, an institution within the governance structure accountable to the executive branch. This model is usually applied in some Asian countries with consideration of the efficiency of policy coordination and the integration of oversight in the governance system. In the Indonesian context, the provisions in the Personal Data Protection Law tend to lead to an executive-based surveillance model. However, to ensure the effectiveness of personal data protection, it is necessary to strengthen functional independence mechanisms and clear arrangements of authority so that supervisory institutions can carry out their duties professionally and free from intervention.

4. CONCLUSION

The establishment of a personal data protection institution, established and determined by the President, and then the provisions described in the Presidential Regulation reflect that the institution cannot be said to be an independent institution because there is still the involvement of executive agency intervention, so that it is not in accordance with the principle of an independent institution. Because in its implementation, this institution could attract the rulers' political interests. Thus, institutions cannot work effectively and efficiently in ensure personal data protection for Indonesian citizens.

REFERENCES

[1] Ackerly, B.A. (2016). Girls are rising for human rights: Not magic, politics. Journal of International Political Theory, 12(1), 26-41. https://doi.org/10.1177/1755088215613626

[2] Anggraeni, SF (2018). Polemic on the Regulation of Personal Data Ownership: The Urgency of Harmonization and Legal Reform in Indonesia. Journal of Law & Development, 48(4), 814. https://doi.org/10.21143/jhp.vol48.no4.1804

[3] Bella Christine, Christine S.T. Chancellor of Finance. (2022) Obstacles to the Implementation of Personal Data Protection in Indonesia after the Enactment of Law Number 27 of 2022 concerning Personal Data Protection. Syntax Literacy: Indonesian Scientific Journal. (7),09. 22-35.Doi:10.36418/syntax-literate.v7i9.13936

[4] Bella Fistya Asherli, & Sidi Ahyar Wiraguna. (2025). Personal Data Security Protection in the Digital Era Facing Phishing Attacks Reviewed from the Personal Data Protection Law Number 27 of 2022. Journal of Law, Public and State Administration, 2(4), 01–14. https://doi.org/10.62383/hukum.v2i4.290

[5] Custers, B., & Malgieri, G. (2022). Valuable data: Why the EU's fundamental right to data protection is at odds with the trade in personal data. *Computer Law and Security Review, 45*, 105683. https://doi.org/10.1016/j.clsr.2022.105683

[6] Fauzie, M.A. (2024). Securing the Future: Indonesia's Personal Data Protection Law and Its Implications for Internet of Things (IoT) Data Privacy. Sriwijaya Crimen and Legal Studies, 2(1), 12. https://doi.org/10.28946/scls.v2i1.3743

[7] Greenleaf, Graham. (2011). Data Privacy Authority Independence: International Standards and the Asia-Pacific Experience. Computer Law & Security Review. 28 (1 & 2). SSRN: https://ssrn.com/abstract=1971627 or http://dx.doi.org/10.2139/ssrn.1971627

[8] Intan, S., Puwa, P., Puluhulawa, F. U., & Rahim, E. I. (2023). PALAR (Pakuan Law Review) is an ideal idea to regulate personal data protection as a form of privacy right in Indonesia. Id. at 100, 25–37. https://doi.org/10.33751/palar.v9i2

[9] Junaedi, A.M. (2025). The Urgency of Personal Data Protection in the Digital Era: An Analysis of Law Number 27 of 2022 concerning Personal Data Protection. Knowledge: Journal of Research and Development Results, 5(2), 247-257. https://doi.org/10.51878/knowledge.v5i2.5269

[10] Lestari, Y., & Mujib, M. M. (2022). Optimizing the Legal Framework for Personal Data Protection in Indonesia (Comparative Law Study). Legal Rules: Journal of Legal Studies, 11(2), 203–234. https://doi.org/10.14421/sh.v11i2.2729