

**JLPH:**
**Journal of Law, Politic
and Humanities**

E-ISSN: 2962-2816
P-ISSN: 2747-1985

<https://dinastires.org/JLPH> dinasti.info@gmail.com +62 811 7404 455

DOI: <https://doi.org/10.38035/jlph.v6i6>
<https://creativecommons.org/licenses/by/4.0/>

Legal Certainty of Personal Data Protection in Indonesia: A Legal Analysis of the Implementation of Law No. 27 of 2022

I Putu Balarama Mahesa Putra¹, Ni Putu Rai Yulianti², Dewa Gede Sudika Mangku³

¹Postgraduate Master of Laws Program, Ganesha University of Education, Indonesia, balarama@student.undiksha.ac.id

²Postgraduate Master of Laws Program, Ganesha University of Education, Indonesia, raiylulianti@undiksha.ac.id

³Postgraduate Master of Laws Program, Ganesha University of Education, Indonesia, sudika.mangku@undiksha.ac.id

Corresponding Author: balarama@student.undiksha.ac.id¹

Abstract: The development of information technology has triggered an increase in incidents of digital data exploitation, prompting the birth of Law Number 27 of 2022 concerning Personal Data Protection (UU PDP) as the main legal instrument (*lex specialis*). This research aims to analyze the legal certainty of personal data protection after the full enactment of the PDP Law and identify juridical obstacles in its implementation in Indonesia. The research method used is normative law (doctrine) with a statutory approach and a conceptual approach. The research results show that the PDP Law has provided a strong normative framework by emphasizing the rights of data subjects, the obligations of data controllers, as well as strict administrative and criminal sanctions. However, the principle of legal certainty is still hampered by the lack of formalization of the independent PDP Authority Supervisory Institution in accordance with the mandate of Article 58, as well as the incomplete completion of several crucial derivative regulations. This condition triggers temporary dualism of supervision and hampers the optimization of corporate sanctions enforcement. This research concludes that accelerating the formation of the Presidential Regulation on PDP Bodies and strengthening the competence of Data Protection Officers (DPO) in each sector is an absolute prerequisite for realizing just legal certainty in Indonesia's digital space.

Keywords: Legal Certainty, Personal Data, Juridical Analysis, PDP Law, Supervisory Institutions

INTRODUCTION

The rapid development of information and communication technology has created various opportunities and challenges. Information technology allows humans to connect with each other without recognizing national borders, so it is one of the driving factors of globalization (Dismukes, J. 2006). Various sectors of life have utilized information technology systems, such as the implementation of electronic commerce (e-commerce) in the

trade/business sector, electronic education (e-education) in the education sector, electronic health (e-health) in the health sector, electronic government (e-government) in the government sector, as well as information technology which is utilized in other fields. The use of information technology makes it very easy for a person's Personal Data to be collected and transferred from one party to another without the knowledge of the Personal Data Subject, thus threatening the constitutional rights of the Personal Data Subject (Gutwirth, S., 2013).

Protection of Personal Data is included in the protection of human rights. Thus, regulations regarding Personal Data are a manifestation of recognition and protection of basic human rights. The existence of a Law on Personal Data Protection is a necessity that cannot be postponed any longer because it is very urgent for various national interests. Indonesia's international community also demands protection of personal data. This protection can facilitate transnational trade, industry and investment (Yulianti, N. P. R., et.al, 2026).

The Law on Personal Data Protection is a mandate from Article 28G paragraph (1) of the 1945 Constitution of the Republic of Indonesia which states that, "Everyone has the right to protection of their personal, family, honor, dignity and property under their control, and has the right to a sense of security and protection from the threat of fear of doing or not doing something which is a human right" (Mangku, et.al. 2022). The issue of Personal Data Protection arises because of concerns about violations of Personal Data that could be experienced by individuals and/or legal entities. These violations can result in material and non-material losses (Admiral, A., & Pauck, M. A. (2023).

The formulation of regulations regarding Personal Data Protection can be understood because of the need to protect the rights of individuals in society regarding the processing of Personal Data both electronically and non-electronically using data processing tools. Adequate protection of Personal Data will be able to provide public confidence to provide Personal Data for various greater societal interests without misuse or violating their personal rights. Thus, this arrangement will create a balance between individual rights and the interests of society whose interests are represented by the state. This regulation on Personal Data Protection will make a major contribution to creating order and progress in the information society (Yulianti, N. P. R., Mangku, D. G. S., & Sariasa, G. (2026).

To reduce overlapping provisions regarding Personal Data Protection, basically the provisions in this Law are standards for the Protection of Personal Data in general, whether processed in whole or in part by electronic and non-electronic means, where each sector can apply Personal Data Protection according to the characteristics of the sector concerned. Personal Data Protection Regulations aim to, among other things, protect and guarantee the basic rights of citizens related to personal protection, guarantee that the public can get services from Corporations, Public Bodies, International Organizations and Governments, encourage the growth of the digital economy and the information and communications technology industry, and support increasing the competitiveness of domestic industries.

Modern social life has shifted towards massive digitalization, where personal data is now being transformed into a very high value economic commodity (the new oil). On the one hand, this phenomenon encourages efficiency in the public service, digital economy, finance and communications sectors. However, on the other hand, vulnerability to data misuse increasingly threatens citizens' right to privacy. Various cases of large-scale data leaks, illegal data trading, and exploitation of digital profiles without consent continue to recur in Indonesia. Before 2022, regulations regarding data protection in Indonesia are still partial and spread across dozens of sectoral laws and regulations, resulting in sectoral egos and legal uncertainty in their enforcement (Itasari, E. R., & Mangku, D. G. S. (2021).

As a concrete response, the government passed Law Number 27 of 2022 concerning Personal Data Protection (UU PDP) on October 17 2022. This regulation is a new milestone because it adopts international standards such as the European Union's General Data Protection

Regulation (GDPR). The government also provides a two-year compliance transition period for industrial players, corporations and public agencies to adjust their data governance.

After the transition period ends, the PDP Law is now fully binding and requires all data controllers to apply the principles of Privacy by Design and Privacy by Default. Normatively, this law presents significant updates, starting from regulating high administrative fines, the threat of imprisonment for individual and corporate perpetrators, to the obligation to appoint a Data Protection Officer (DPO).

Even though formal legal instruments are available, the reality on the ground shows inequalities that harm the principle of legal certainty (*rechtssicherheit*). The main obstacle stems from the lack of operation of an independent PDP Authority Supervisory Institution as mandated by Article 58 paragraph (2) of the PDP Law. The absence of this independent institution has implications for unclear incident reporting mechanisms, overlapping temporary monitoring functions, and slow execution of fair sanctions for victims. Referring to these juridical dynamics, this research formulates two main issues: What is the legal certainty of personal data protection in Indonesia after the enactment of Law no. 27 of 2022 in full? And what are the juridical obstacles in implementing law enforcement of Law no. 27 of 2022 regarding current cases of personal data breaches?.

METHODS

This research uses a type of normative legal research, which is often referred to as doctrinal legal research or library research. The main focus of normative legal research is studying law written in books and analyzing abstract legal norms contained in statutory regulations. The nature of this research is descriptive-analytic. This research aims to describe comprehensively, systematically and accurately the implementation and legal certainty of Law no. 27 of 2022 concerning Personal Data Protection (PDP Law), then analyzes the juridical obstacles that arise due to the non-operationalization of the PDP Authority Supervisory Agency in Indonesia (Khan, A. N., 2023).

To solve the problem formulation and produce a sharp juridical analysis, this research combines two types of legal approaches, namely: Statute Approach: This approach is carried out by examining all regulations and legislation that are related to the legal issue being researched. Researchers examine the normative consistency, hierarchy and binding force of the PDP Law, ITE Law no. 1 of 2024, to Article 28G of the 1945 Constitution. Conceptual Approach: This approach departs from doctrines, expert views and legal concepts that develop in cyber law. Researchers use the theory of legal certainty (*rechtssicherheit*), the principle of Privacy by Design, and the concept of independence of state law enforcement agencies to dissect the problem of the vacuum of PDP Authority (Gawas, V. M. (2017).

The collection of legal materials in this research was carried out through the library research method. Researchers carry out inventory, categorization and recording of legal documents, both in physical and digital form (e-resources). The process of searching for digital legal materials utilizes official government databases (such as JDIH BPK, JDIH Ministry) and scientific journal portals (such as Google Scholar and Sinta). The legal materials that have been collected are analyzed using qualitative methods with normative deductive techniques. Researchers carry out legal interpretation using systematic interpretation and teleological (sociological) interpretation to see the suitability between the text of the law and the aim of protecting citizens' rights in the field. The process of drawing conclusions is carried out deductively, namely drawing conclusions from general premises (the theory of legal certainty and the regulatory text of the PDP Law) to specific matters (obstacles to law enforcement due to the absence of a PDP Authority Supervisory Agency) (Elihami, E. (2024).

RESULTS AND DISCUSSION

Juridical Analysis of Legal Certainty for Personal Data Protection Post Full Implementation of Law no. 27 of 2022

The principle of legal certainty (*rechtssicherheit*) demands that the law must be clear, enforceable, and provide consistent protection for legal subjects. The end of the two-year transition period in October 2024 marks a new phase where Law Number 27 of 2022 concerning Personal Data Protection (UU PDP) is fully binding on all legal subjects in Indonesia, both private corporations, digital platforms and public agencies (Maulana; 2026).

Theoretically-normatively, the presence of the PDP Law succeeded in ending the era of fragmentation of personal data regulations which were previously spread sectorally across dozens of separate regulations. The PDP Law exists as a *lex specialis* which brings several significant legal reforms to ensure substantive legal certainty:

- **Codification of Data Subject Rights:** Articles 5 to 14 of the PDP Law explicitly detail the rights of personal data owners. These rights include the right to obtain information, correct data errors, end processing, and the right to delete data (right to be forgotten). This standardization provides certainty for citizens regarding what digital constitutional rights they have.
- **Obligations of Data Controllers:** This law imposes absolute responsibility on Personal Data Controllers (Data Controllers) and Personal Data Processors (Data Processors). Based on Article 26 of the PDP Law, if a protection failure occurs (data leak), the data controller is obliged to provide official written notification within a maximum of 3 x 24 hours to the personal data subject and the supervisory institution.
- **Progressive Dualism of Sanctions:** The PDP Law provides two law enforcement instruments at once. Administrative sanctions are regulated in the form of fines of up to 2% of the annual income of the violator's total turnover (Article 57). Meanwhile, criminal sanctions (Article 65 and Article 66) threaten corporate and individual perpetrators with prison sentences of up to 6 years and criminal fines of billions of rupiah for illegal acts such as falsifying or trading personal data.

Normatively, the PDP Law has fulfilled the prerequisites for legal certainty in terms of the availability of legal substance. However, legal certainty does not just stop at ratifying written rules, but is also determined by how these rules can be operationalized effectively in the field (legal enforcement).

Juridical Obstacles in Implementation and the Impact of Vacancies in the PDP Authority Supervisory Institution

Even though the material basis of the law is fully binding, law enforcement of the PDP Law still faces crucial juridical obstacles. The most fundamental obstacle stems from the institutional vacuum due to the lack of formalization of the Personal Data Protection Authority Supervisory Agency (PDP Agency) (Putri; 2025).

Based on the mandate of Article 58 paragraph (2) of the PDP Law, this Supervisory Agency is an independent institution appointed directly by the President to carry out policy formulation, ecosystem monitoring and cyber administrative law enforcement. Current institutional conditions trigger three main juridical problems:

1. **Overlapping Temporary Supervision:** As long as the Presidential Regulation (Perpres) on institutions has not been ratified, the function of supervising digital space governance is still handled transitionally by the Directorate General of Digital Space Supervision under the Ministry of Communication and Digital (Komdigi). This is considered to trigger a juridical conflict of interest if the data leak incident actually occurs on a platform or institution belonging to the government agency itself. Ideally, supervisory institutions must stand independently in order to be objective in judging the private and public sectors.

2. Absence of Technical Guidelines for Administrative Fines: Article 61 of the PDP Law confirms that procedures for implementing institutional authority are regulated through Government Regulations (PP). Because the implementing PP and institutional Presidential Decree are still in the final harmonization stage, the criteria for calculating administrative fines of 2% do not yet have a clear operational reference. As a result, enforcement of sanctions against private corporations that violate data cannot be executed optimally and optimally.
3. Uncertainty of Dispute Resolution Mechanisms: Data owners who are harmed by cases of mass data leaks experience difficulties in taking official administrative complaint routes. A special arbitration channel or data dispute adjudication board under the PDP Agency does not yet exist, so the public is forced to use the usual Unlawful Act (PMH) lawsuit instrument through Article 1365 of the Civil Code or report it as a general criminal act, the electronic proof process of which takes a long time.

These juridical obstacles led to a lawsuit for judicial review at the Constitutional Court by civil society groups in mid-2026. The lawsuit demands certainty about the deadline for the formation of the PDP Agency because the delay in the operationalization of the supervisory institution is considered to be infringing the right to fair legal certainty in accordance with Article 28D paragraph (1) of the 1945 Constitution.

Even though the government emphasizes that there is no legal vacuum because the substance of the PDP Law remains binding, accelerating the issuance of the Presidential Decree on PDP Institutions and the PP on sanctions is a prerequisite that cannot be postponed any longer in order to enforce effective enforcement of the privacy protection ecosystem in Indonesia.

CONCLUSIONS AND RECOMMENDATIONS

Conclusion

Based on the results of the juridical analysis and discussions described in the previous chapters, this research concludes two basic things:

1. Legal certainty after the enactment of Law no. 27 of 2022: Ratification of the PDP Law has normatively succeeded in ending the era of fragmentation of data protection law in Indonesia by positioning itself as a *lex specialis*. This law provides certainty in the aspect of dismantling past laws through standardization of data subject rights, strict obligations of data controllers, as well as progressive classification of administrative fines and criminal sanctions. However, material (practical) legal certainty has not been fully realized in society because the formal operational instruments have not run optimally.
2. Juridical Obstacles in Implementation: The main legal obstacle in enforcing the PDP Law is the institutional vacuum due to the lack of formalization of the independent PDP Authority Supervisory Agency under the President. This condition triggers unclear law enforcement flows, overlapping sectoral supervision, and hampers the centralized execution of administrative sanctions. Apart from that, the unfinished Government Regulations (PP) and Presidential Regulations (Perpres) as implementing derivative regulations mean that the regulations for corporate fines and the mechanism for appointing Data Protection Officers are still losing their technical ground in the field.

RECOMMENDATIONS

In order to realize the principle of legal certainty that is just, certain and effective in the Indonesian digital ecosystem, the following strategic points are recommended:

1. Accelerate the Establishment of an Independent Supervisory Agency: The President together with the Ministry of Communication and Digital must immediately finalize and ratify a Presidential Regulation regarding the structure, function and working procedures

of the Personal Data Protection Authority. This institution must maintain its independence from political and industrial intervention so that it can act objectively in examining public and private agencies that commit data breaches.

2. Acceleration of Derivative Regulations (PP and Presidential Decree): The government needs to prioritize the issuance of Government Regulations that regulate procedures for calculating administrative fines as well as formal mechanisms for resolving personal data disputes. This is crucial so that law enforcement officials and supervisory institutions have technical guidance that is uniform, explicit and free from multiple interpretations of the law.
3. Standardization of Public and Private Sector Compliance: Every government agency and medium-large scale corporation is advised to immediately carry out mandatory technology audits and appoint an officially certified Data Protection Officer (DPO). Massive outreach regarding the rights of data subjects must also be increased so that the public is able to mitigate risks and understand the legal recourse when their privacy rights are violated.

Acknowledgment

The author wishes to express sincere gratitude to Prof. Dr. Dewa Gede Sudika Mangku, S.H., LL.M. and Dr. Ni Putu Rai Yulianti, S.H., M.H. of the Postgraduate Program, Universitas Pendidikan Ganesha, for invaluable guidance, rigorous supervision, and critical feedback throughout the development of this article. Appreciation is also extended to the anonymous reviewers whose comments contributed substantially to the refinement of the argument advanced in this study, and to the editorial team of Journal of Law, Politics, and Humanities for their professional handling of the manuscript. Any errors or omissions remain the sole responsibility of the author.

REFERENCES

- Admiral, A., & Pauck, M. A. (2023). Unveiling the Dark Side of Fintech: Challenges and Breaches in Protecting User Data in Indonesia's Online Loan Service. *Lex Scientia Law Review*, 7(2), 995-1048. 10.3280/RISS2024-002017
- Devi, P. F. S., Mangku, D. G. S., & Yulianti, N. P. R. (2026). Legal Protection of Children's Privacy Rights from Global EdTech Governance Oversight. *proceedings. icesy*, 1(01).
- Gawas, V. M. (2017). Doctrinal legal research method a guiding principle in reforming the law and legal system towards the research development. *International Journal of Law*, 3(5), 128-130.
- Gellert, R., & Gutwirth, S. (2013). The legal construction of privacy and data protection. *Computer Law & Security Review*, 29(5), 522-530.
- Itasari, E. R., & Mangku, D. G. S. (2021). Legal Protection Against Violations of Human Rights That Abuse Uighur Ethnic Women in China. *Yinyang: Jurnal Studi Islam Gender Dan Anak*, 33-48.
- Majeed, N., Hilal, A., & Khan, A. N. (2023). Doctrinal research in law: Meaning, scope and methodology. *Bulletin of Business and Economics (BBE)*, 12(4), 559-563. <https://doi.org/10.61506/01.00167>
- Mangku, D. G. S., Yulianti, N. P. R., & Hadi, N. G. A. H. (2022, September). Digital contact tracking as a prevention of Covid-19 and the problem of data privacy protection. In *AIP Conference Proceedings* (Vol. 2573, No. 1, p. 020011). AIP Publishing LLC. <https://doi.org/10.1063/5.0104104>
- Maulana, M. I. A., Yulianti, N. P. R., & Mangku, D. G. S. (2026). Evaluasi Implementasi Undang-Undang Perlindungan Data Pribadi pada Kasus Kebocoran Data Pengguna E-Commerce di Indonesia: (Studi Kasus Perlindungan Data Pribadi). *Hukum Inovatif: Jurnal Ilmu Hukum Sosial dan Humaniora*, 3(2), 41-51.

- Miller, L., Miller, R., & Dismukes, J. (2006). The critical role of information and information technology in future accelerated radical innovation. *Information Knowledge Systems Management*, 5(2), 63-99.
- Putri, H. A. (2025). Legal Review of the use of Personal Data in the Development of Artificial Intelligence Under the Personal Data Protection Law. *Jentera: Jurnal Hukum*, 6(1), 1-15.
- Rohman, M. M., Mu'minin, N., Masuwd, M., & Elihami, E. (2024). Methodological reasoning finds law using normative studies (theory, approach and analysis of legal materials). *MAQASIDI: Jurnal Syariah dan Hukum*, 204-221.
- Yulianti, N. P. R., Mangku, D. G. S., & Sariasa, G. (2026). From algorithms to crime: A criminal law analysis of the use of bots to manipulate public opinion. *BIS Humanities and Social Science*, 4, V426006-V426006. 4, <https://doi.org/10.31603/bishss.433>