Journal of Law & Social Politics
Volume 4, Issue 6, 1506-1516
e_ISSN: 2807-6311
https://jolastic.id/index.php/jlsp/index
DOI: doi.org/10.59261/jlsp.v4i6.161

Legal Protection of Citizens' Personal Data A Case Study on Law No. 27 of 2022

Edi Ribut Harwanto[1]* Universitas Muhammadiyah Metro, Indonesia
Azmi Syahputra[2] Universitas Trisakti, Indonesia

***Corresponding author:**
Edi Ribut Harwanto, Universitas Muhammadiyah Metro, Indonesia.
✉edilaw5863@gmail.com

Article Info:
***Article history*:**
Received: June 06, 2026
Revised: October 27, 2026
Accepted: July 29, 2026
Available Online: November 17, 2026

***Keywords*:**
California Consumer Privacy Act;
General Data Protection Regulation;
Personal Data Protection Law;
Privacy Rights;
Public Awareness;

This is an open access article under the CC BY-SA license.

Copyright © 2026 by Author. Published by Politeknik Siber Cerdika International

Abstract

Background: The enactment of Law No. 27 of 2022 on Personal Data Protection (PDP Law) represents Indonesia's commitment to safeguarding personal information and ensuring legal certainty. However, limited public awareness, inadequate understanding among law enforcement officials, and resource constraints continue to hinder its implementation.
Objective: This study aims to examine the implementation of the PDP Law, identify enforcement challenges, and assess public awareness of personal data protection rights and criminal sanctions.
Methods: This study employed a systematic data collection approach combining quantitative and qualitative descriptive analyses, including interviews and surveys.
Results: The findings indicate persistent challenges in enforcing personal data protection regulations in Indonesia, particularly compared with international frameworks such as the European Union's General Data Protection Regulation (GDPR) and California's Consumer Privacy Act (CCPA). Interviews revealed that seven out of ten informants identified the absence of an independent supervisory authority as the primary enforcement obstacle. Furthermore, survey results showed that only 34% of respondents were aware of their right to data erasure under the PDP Law, highlighting significant gaps in public legal awareness.
Conclusion: Effective implementation of the PDP Law requires stronger law enforcement, independent supervisory institutions, regulatory improvements, and comprehensive public education. Strengthening these measures is essential to enhancing personal data protection, ensuring legal certainty, and aligning Indonesia's regulatory framework with international standards.

To cite this article: Harwanto, E. R. & Syahputra, A. (2026). Legal protection of citizens' personal data: A case study on Law No. 27 of 2022. *Journal of Law & Social Politics*, *4*(6), 1506-1516. https://doi.org/10.59261/jlsp.v8i6.161

INTRODUCTION

Rapid Development of Information and Communication Technology in Indonesia Enters the Top 10 Largest Data Leaks: The 2024 report shows that Indonesia is included in the list of 10 countries with the highest level of personal data leaks in the world. Hundreds of Cases Handled by the Ministry of Communication and Information: The Ministry of Communications and Digital (formerly the Ministry of Communication and Information) handled 111 cases of personal data leaks from 2019 to May 2024. Large-Scale Leaks: Several large cases affected government and public agencies, such as the National Data Center data leak (June 2024), passport data of 35 million Indonesian citizens (2023), and BPJS Health data. Massive Cyber Attacks: BSSN recorded trillions

of cyber attacks in the first half of 2025, indicating a very high threat to data infrastructure. System Weaknesses: Many cases of data leaks are caused by low system security factors, where sensitive data is often stored without encryption (Hukum et al., 2023).

Implementation of the PDP Law: Even though Law Number 27 of 2022 concerning Personal Data Protection (UU PDP) is fully in force, its enforcement still faces challenges because a special supervisory institution will not be fully formed until early 2025. This study aims to: (1) analyze the normative framework of Law No. 27 of 2022 and identify gaps in its implementation provisions; (2) assess public awareness levels and institutional readiness for enforcement through empirical data; and (3) propose evidence-based policy recommendations for strengthening personal data protection in Indonesia. Information and communication technology (ICT) has brought major changes to human life, especially in terms of how to interact, work and communicate. Since the emergence of the internet, digital technology has developed very quickly, allowing instant access to information and without geographical restrictions.

Technologies such as artificial intelligence (AI), internet of things (IoT), big data and cloud computing are now used in various sectors, providing convenience but also posing big risks regarding the protection of personal data (Ahmad et al., 2022; Pathak et al., 2024). More and more personal data is being collected through digital transactions, social media use, and mobile applications that can be used for a variety of purposes (Iman, 2024; Polykalas & Prezerakos, 2019). A critical review of existing studies reveals significant gaps. Bangsu et al. (2026) examined data controller obligations under the PDP Law but focused exclusively on normative provisions without assessing implementation effectiveness. Alhazmi et al. (2024) applied the GDPR framework but did not address the specific Indonesian institutional context. Morgan et al. (2022) analyzed digital literacy without systematically connecting awareness levels to specific legal provisions. These studies demonstrate the absence of integrated normative-empirical research examining the PDP Law's enforcement gap and public awareness deficit. This data is often used for consumer behavior analysis and advertising personalization, but without adequate regulation, this personal data can be misused (Budiman, 2024).

Protection of privacy rights in the digital era faces major challenges, especially in terms of regulating and monitoring the use of personal data (Politou et al., 2021; Renuka et al., 2024; Romansky & Noninska, 2020). Often, personal data collected through various digital platforms is used without the consent or clear understanding of the individual concerned (Cain & Imre, 2022; Kreuter et al., 2020). Many digital apps and services are not transparent about how their personal data will be used, increasing the potential for privacy violations (Betzing et al., 2020; Quach et al., 2022). One example that often occurs is data leaks involving large companies, which result in consumer personal data being used for fraudulent or exploitative purposes (Mada, 2024).

The inhibiting factors that need to be improved in the grant fund monitoring system in Indonesia are the lack of strict supervision and the limited resources available to handle cases of personal data breaches. In Indonesia, even though the Personal Data Protection Law (UU PDP) has been passed, its implementation still faces many obstacles. One of the main problems is the lack of public understanding of their rights regarding the protection of personal data. Many individuals are unaware of the importance of control over their personal data or how their data is used by companies. This shows that even though there are existing regulations, their implementation is still not optimal, and many individuals are still vulnerable to misuse of personal data.

The Importance of Personal Data Protection as Part of Human Rights. The right to privacy is an important part of internationally recognized human rights. In the Universal Declaration of Human Rights (UDHR), which was ratified by the UN in 1948, Article 12 states that "no one shall have his privacy, his family, his home, or his papers invaded. In addition, the International Covenant on Civil and Political Rights (ICCPR) also underlines the right of every individual to be protected from unauthorized interference with his privacy. In the digital era, personal data has become increasingly vulnerable to misuse. Personal data protection is not only about safeguarding sensitive information, but also about protecting individual freedom from unlawful surveillance. Without adequate protection, individuals may become victims of identity theft or behavioral manipulation. This protection is also important for building public trust in digital technology. If individuals feel that their personal data is not protected, they will be reluctant to

use digital platforms, which can hinder the development of the digital economy and the progress of society as a whole (Siddiqui & Farooqi, 2024).

Global Challenges in Personal Data Protection in Indonesia. Apart from the challenges faced by Indonesia, personal data protection is also a big issue being faced globally. Countries around the world are currently trying to formulate appropriate regulations to regulate the use of personal data in this digital era. However, despite many initiatives, differences in regulation and law enforcement between countries often create loopholes that allow misuse of personal data. Each country has a different approach to personal data protection, which often depends on the legal, social and economic conditions of each country. For example, in Europe, the General Data Protection Regulation (GDPR) is one of the strictest regulations in the world in terms of personal data protection (Saly et al., 2023).

GDPR regulates the rights of individuals regarding their personal data by giving users greater control over their data, as well as imposing heavy sanctions on companies that violate this regulation. However, although GDPR provides high standards for personal data protection in Europe, many developing countries still lag behind in terms of regulation.In these countries, the implementation of personal data protection is still very limited due to limited resources, legal knowledge and infrastructure that supports the implementation of these regulations. This regulatory regulation is a big challenge due to the nature of personal data as it crosses national borders. Personal data collected by multinational companies, for example, can easily move from one country to another without taking into account the personal data protection laws that apply in the country where the data originates (Imran, 2024).

This becomes a big problem, especially when the data that crosses these borders is not adequately protected or is used for unauthorized purposes. In many cases, companies operating in different countries over time choose to follow looser regulation, which allows them to avoid the costs and more stringent obligations imposed by regulation in countries with stronger protection.In balanced countries, including Indonesia, although there have been efforts to carry out personal data protection regulations, there are still many aspects that need to be improved. One of the biggest challenges is effective law enforcement. In many countries, institutions tasked with monitoring and enforcing personal data protection laws increasingly do not have sufficient resources to handle increasingly complex cases of data breaches or leaks. Apart from that, there are still many people who are not fully aware of the importance of protecting personal data and their rights in the digital world.

This leads to information inequality between users and providers of digital services. Success in implementing personal data protection regulations in one country often depends on international cooperation, considering the cross-border nature of data. For example, companies that operate in many countries must comply with various regulations that exist in each country, but this can be difficult if there is no international agreement that regulates how personal data must be protected. Therefore, it is important for countries in the world to strengthen international cooperation in creating more harmonious and effective regulation in the protection of personal data. One important initiative is through the establishment of international standards that can be adopted by countries, both developed and balanced, to address the problem of misuse of personal data (Barati, 2023).

METHOD

This study employs a normative-empirical legal research method (socio-legal research) using a mixed-methods approach, which combines qualitative and quantitative data. The normative research is used to examine the legal norms governing personal data protection, specifically the provisions of Law No. 27 of 2022 on Personal Data Protection (UUDP). Meanwhile, the empirical research is used to analyze the implementation of these norms in practice in the digital age. The research approaches used include the Statute Approach, which examines laws and regulations related to personal data protection; the Conceptual Approach, which examines the concepts of legal protection, the right to privacy, data security, and exceptions to the use of personal data; and the Case Approach, to analyze cases of personal data use that fall under the exceptions outlined in the Personal Data Protection Act (UUDP), and the Sociological Approach, to assess the effectiveness of the UUDP Data collection was conducted through three instruments:

(1) Semi-structured interviews with 10 key informants, comprising 3 data protection officers from private sector companies, 3 government officials from the Ministry of Communications and Digital, 2 civil society representatives, and 2 legal practitioners specializing in data protection law, selected through purposive sampling based on their direct involvement in PDP Law implementation; (2) Non-participant observation of data protection compliance practices at 5 electronic system operators in Jakarta during January-March 2025; and (3) Documentary analysis of regulatory texts, institutional reports, and court decisions related to personal data breaches. Quantitative data were collected through an online survey distributed to 200 respondents across five major Indonesian cities (Jakarta, Surabaya, Bandung, Medan, and Makassar) using stratified random sampling, with a response rate of 78% (n=156). Data validation was ensured through methodological triangulation, cross-referencing interview findings with documentary evidence and survey results. Qualitative data were analyzed using thematic analysis following Braun and Clarke's (2006) six-phase framework, while quantitative data were analyzed using descriptive statistics.'s implementation in society and the operation of electronic systems (Hukum et al., 2023).

RESULTS AND DISCUSSION

Results

The effectiveness of the Personal Data Protection Act No. 27 of 2022, enacted in 2022, lies in the extent to which entities that manage personal data (in both the public and private sectors) comply with its provisions through the implementation of effective policies and adequate oversight regarding the enforcement of personal data protection. Due to limitations in legal infrastructure and resources, data controllers are not yet fully aware of the potential risks or legal consequences of leaks involving the personal data they manage. One solution to this problem is through more extensive and integrated educational campaigns that emphasize the importance of personal data protection.

The results of this qualitative study are presented in the form of a description of the application of exceptions to the use of personal data under Law No. 27 of 2022 on Personal Data Protection. They cover stakeholders' understanding of personal data protection, challenges in implementing legal norms, and the effectiveness of oversight and law enforcement. These findings were obtained from in-depth interviews, observations, and document analysis. Interview data were analyzed through data reduction, thematic categorization, data presentation, and conclusion drawing, while the results of observations and documentation were used to strengthen and verify the research findings through triangulation.

Meanwhile, the results of the quantitative research are presented in the form of annual curves illustrating the development of personal data protection and the implementation of Law No. 27 of 2022 on Personal Data Protection from year to year. These curves are used to show changes in the number of personal data breach cases, the compliance rates of electronic system operators, public awareness levels, and the effectiveness of law enforcement following the enactment of the Personal Data Protection Act (UUDP), Among them are the following, among others:

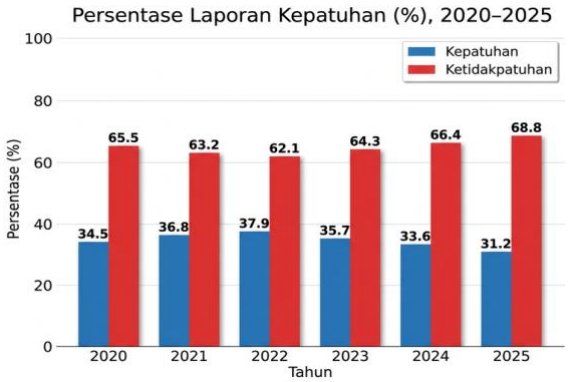


Figure 1. Respondents' experiences regarding the use of personal data without consent (%) from 2020 to 2025
(Source: Online survey, n=156, collected January-March 2025 using stratified random sampling across five major Indonesian cities. Data analyzed using descriptive statistics.)

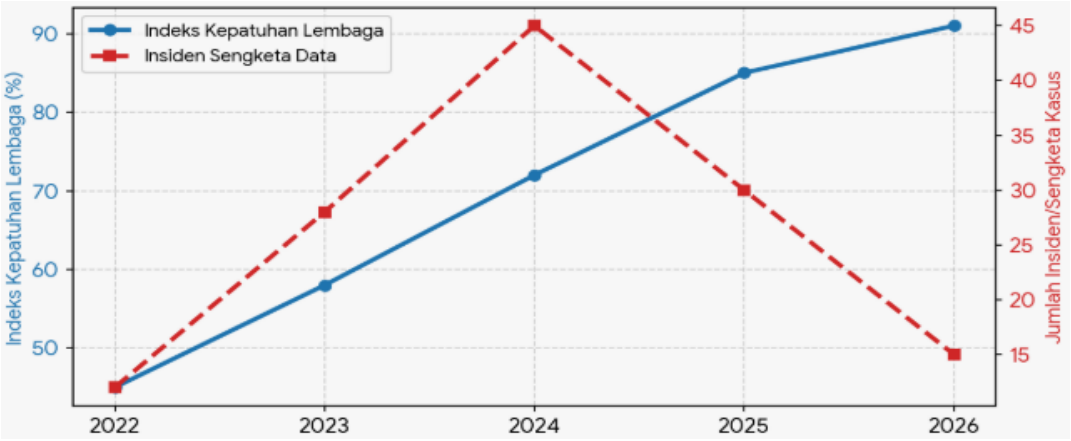


Figure 2. The Curve of Protection and Compliance with Exempted Personal Data: A Case Study of Law No. 27 of 2022 to 2026

Discussion

Concept of the Right to Privacy

Understanding the Right to Privacy in the Legal Context of the Personal Data Law in Indonesia

The right to privacy refers to an individual's right to protect himself from unauthorized inteirvein, especially in the case of personal information. In a legal context, the right to privacy covers various dimensions, such as protection of personal life, correspondence, communications and personal data. In the legal systems of many countries, this right is recognized as a fundamental human right. Protection of the right to privacy is very important to maintain individual freedom in determining what other people can or cannot know about themselves. The right to privacy is becoming increasingly relevant in the digital world, where the collection and distribution of personal data can occur quickly and without the explicit consent of the individuals concerned (Imran, 2024).

The Relevance of Privacy Rights in Digital Era Life

In the digital era, the right to privacy has enormous relevance because technology allows personal information to be collected, processed, and shared in ways that have never been possible before. Digital platforms such as social media, data-based applications, and e-commerce collect users' personal data for various purposes, both legitimate and not. This collected data is then used to create profiles, behavioral analysis and highly personalized advertising. Without adequate protection, this personal data can be misused for various purposes, such as behavioral manipulation or even identity theft. Therefore, protecting the right to privacy has become a very important aspect in maintaining a balance between technological progress and protecting human rights in digital life (Putri et al., 2025).

Personal Data Protection Regulations in Indonesia

Law No. 27 of 2022 concerning Personal Data Protection (UU PDP) as a Juridical Basis for Personal Data Protection in Indonesian Society

In Indonesia, personal data protection has begun to be regulated more clearly with the passing of the Personal Data Protection Law (UU PDP) in 2022. This law is designed to provide legal protection for individual personal data, both within the country and involving individuals from outside the country who interact with the system that has evolved in Indonesia. This law regulates the obligations of personal data managers, both government and private institutions, to protect the personal data they collect. The PDP Law also provides strict sanctions for parties who violate the rules regarding the management of personal data. This law shows Indonesia's progress in overcoming the challenges posed by increasingly rapid advances in information technology, especially regarding the collection and use of personal data online (Siddiqui & Farooqi, 2024).

Discussion of the Concept and Scope of the Personal Data Protection Law

The main concept of the PDP Law is to provide individuals with protective rights over their personal data. In this law, every individual has the right to know, access, correct and delete their

personal data stored by other parties. In addition, personal data controllers are also required to obtain clear and explicit consent from individuals before collecting or processing personal data. The scope of the PDP Law covers personal data collected by various parties, whether by companies, government institutions, or digital service providers. This law also regulates procedures for processing personal data which must be carried out in a transparent and accountable manner, as well as giving individuals complete control over their data. This law guarantees that personal data will not be misused for illegal purposes (Saly et al., 2023).

Privacy Protection in the Digital Era

Challenges and Risks of Privacy Violations in the Digital World

Violations of privacy in the digital world are becoming an increasingly complex problem, especially because a lot of personal data is collected without explicit consent or sufficient understanding from the individual. One of the biggest challenges is the massive collection of personal data by companies without sufficient transparency regarding how this data is used. The biggest risk of collecting data without adequate protection is data leakage, where personal information that should be protected can be spread to unauthorized parties. Apart from that, there is also misuse of personal data for purposes that are detrimental to individuals, such as manipulating consumer behavior or identity theft. Cases such as the Facebook data leak in 2018 and the misuse of data by the company Cambridge Analytica show how big the risks faced by individuals are regarding digital privacy (Mada, 2024).

Cases of Privacy Violations in the Digital World

The most famous example of privacy violations in the digital world is the Facebook data leak case which involved more than 50 million users whose data was used without their permission for political purposes by Cambridge Analytica. This case raises serious questions about how personal data can be used without clear controls and how existing regulations are not strong enough to prevent abuse. Another relevant case is data leakage involving health service providers or e-commerce platforms which often do not take privacy policies seriously. These companies often fail to ensure that the data they collect is properly protected, resulting in privacy breaches that harm individuals (Budiman, 2024).

Legal Protection of Personal Dat

Legal Basis of the Personal Data Protection Law

Background and Urgency of the Establishment of the Personal Data Protection Law

The Personal Data Protection Law was created to provide legal guarantees for individuals regarding the protection of personal data in the era of rapid technological balance. The guidance of the PDP Law is very important, considering that personal data is now a very valuable asset in the digital world, but is also very vulnerable to misuse. With this law, it is hoped that individuals will be better protected and can control their medical data better. The urgency of implementing the PDP Law becomes increasingly clear considering the many cases of misuse of personal data that have occurred in the last few years, both by companies and irresponsible third parties. This law provides a strong legal basis for regulating how personal data must be managed, as well as providing clear sanctions for parties who violate these regulations.

Scope of Personal Data Protection in This Law

The PDP Law covers all types of personal data collected by data companies, whether carried out by public or private sectors. This law stipulates that data managers must obtain explicit consent from individuals before collecting or processing personal data. In addition, individuals have the right to access and correct personal data held by data managers. The PDP Law also provides individuals with the right to delete personal data that has been collected by data management companies, as well as regulating how such data can be processed for legitimate purposes and in accordance with applicable regulations. With a clear scope in the PDP Law, it is hoped that individual privacy rights can be better protected in the digital world (Putri et al., 2025).

Substance of the Personal Data Protection Law

Individual Rights in Personal Data Protection According to the PDP Law

The PDP Law provides various rights for individuals regarding Meireika's personal data. One of the most important rights is the right to access information about personal data held by

other parties, as well as the right to correct or delete such data if it is inaccurate. In addition, individuals also have the right to withdraw Meireika's consent for the processing of personal data at any time, which gives the individual complete control over Meireika's data. The PDP Law also regulates individuals' rights to report if their personal data is misused or leaked, as well as to obtain appropriate redress.

Obligations of Personal Data Managers

Personal data managers, both public institutions and private companies, have an obligation to safeguard the personal data they collect in a safe manner and in accordance with existing regulations. Meireika shall implement adequate security measures to protect data from leakage and misuse. Data managers must also ensure that personal data is only used for legitimate purposes and has been approved by the individual. Meireika must be transparent about its privacy policy and provide clear information about how the data will be used (Saly et al., 2023).

Sanctions and Law Enforcement Mechanisms in the PDP Law

The PDP Law stipulates quite stringent sanctions for data handlers who violate personal data protection requirements. These sanctions include fines which can reach billions of rupiah and imprisonment for violators who are proven to have intentionally committed the violation. The legal enforcement mechanisms contained in this Law also include oversight carried out by the host institutions to ensure compliance with personal data protection regulations, as well as providing a way for individuals to file claims if their rights are violated. Below is a deeper and more detailed description regarding the points you requested, as well as the addition of relevant footnotes (Imran, 2024).

Application for Implementation of the Personal Data Protection Law

Effectiveness of Implementation of the Personal Data Protection Law

Discussion about the extent to which the PDP Law has been implemented by law enforcement officials (APH) and the Indonesian publicThe Personal Data Protection Law No. 27 of 2022, which was passed in 2022, is a big step in regulating and protecting personal data in Indonesia. However, although this law provides more comprehensive protection for personal data, its implementation still faces various challenges. One of the important indicators of the effectiveness of this law is the extent to which the parties managing personal data (both public and private sectors) comply with the provisions contained in the law. One aspect that is still a major task is the implementation of effective policies and adequate supervision regarding the implementation of personal data protection.

At the beginning of its implementation, there were still many private sectors, including digital platforms, that did not fully comply with existing regulations. Many applications and companies still have not updated Meireika's privacy policies in accordance with the PDP Law or are not even transparent enough in terms of how Meireika's personal data is processed. The PDP Law requires data administrators to obtain explicit consent from individuals before the data is collected, but oversight of this is still weak. This shows that even though the PDP Law has been formally implemented, its implementation is still limited, and many sectors must be encouraged to comply more with existing regulations (Mada, 2024).

Obstacles Faced in Implementing the PDP Law, some of the obstacles in implementing the PDP Law are related to limited legal infrastructure and resources. One of the biggest challenges is monitoring personal data protection policies that are not yet operating optimally. Supervisory institutions, such as the Personal Data Protection Commission, have limited powers in terms of monitoring institutions or companies that collect personal data. Apart from that, the lack of legal enforcement regarding violations committed by data management parties, which do not have sufficiently binding or effective sanctions, is also a big problem.

On the other hand, another problem that is being faced is the lack of understanding or skills among data managers to follow applicable rules. Many data managers, both in the private and public sectors, do not yet have adequate systems to protect personal data. This lack of training and outreach to data managers hampers the effective implementation of the PDP Law. In many cases, data managers are not fully aware of the potential risks or legal consequences of leaking the personal data they manage (Saly et al., 2023).

Analysis of Challenges in Implementing the Personal Data Protection Law

Public Awareness Issues Regarding Privacy Rights

Public awareness of privacy rights and personal data protection in Indonesia is still strong. Many individuals do not fully understand Meireika's rights regarding the management of Meireika's personal data. The public often does not realize that Meireika has the right to access, correct and delete Meireika's personal data that has been collected by companies or other institutions. This is caused by a lack of education and outreach regarding personal data protection, both from the government and the private sector.

The lack of information about privacy rights causes society to increasingly give its consent to data management without fully understanding how their data will be used or misused. In addition, many internet users are not aware of the risks arising from data leaks, so they are not careful enough in sharing their personal information in cyberspace. One solution to this problem is through a more massive and integrated education campaign that emphasizes the importance of protecting personal data. This campaign must include an understanding of the rights that individuals have and how Meireika can protect Meireika's personal data (Siddiqui & Farooqi, 2024).

Legal and Technical Barriers in Enforcing Personal Data Protection Laws, apart from the problem of public awareness, there are obstacles to effective law enforcement regarding the protection of personal data. Many companies and data management institutions have not yet complied with the requirements of the PDP Law. This occurs due to a lack of systematic oversight and the absence of a complaint mechanism that is easily accessible to the public. Supervision carried out by institutions such as the Personal Data Protection Commission is still limited in terms of capacity and authority.

On the technical side, another problem is that many personal data management systems do not yet meet adequate security standards. Poor cyber security or the absence of a clear data management system increases the risk of data leaks that could harm individuals. This happens because data management does not always follow the technical standards that have been set by regulation or does not have an adequate system to mitigate existing risks. Therefore, better training is needed for data managers as well as increasing the capacity of supervisory institutions so that they can enforce the PDP Law more effectively (Hukum et al., 2023).

The Role of Supervisory Institutions to Ensure Personal Data Protection. Supervisory institutions that have a key role in ensuring the effective implementation of personal data protection must be provided with greater capacity and independence in carrying out their duties. Institutions such as the Personal Data Protection Commission need to be strengthened in terms of their resources and authority to carry out audits of data management by personal data administrators. In addition, supervisory institutions must have clear and firm mechanisms for handling reports and complaints regarding violations of personal data protection. This capacity limitation means that supervisory institutions cannot work optimally, so that violations of personal data are difficult to deal with properly. Therefore, it is important to increase the capacity of these supervisory institutions through increasing budgets, trained human resources and advanced technology (Budiman, 2024).

Comparison of the Implementation of UUDP Law with Other Countries

Comparison of Personal Data Protection Regulations in Indonesia with Other Countries (For example: GDPR in Europe, CCPA in California, etc.). A comparison of the Indonesian PDP Law with existing personal data protection regulations in other countries, such as Global Data Protection Regulation (GDPR) in Europe and the California Consumer Privacy Act (CCPA) in California, shows several significant differences. GDPR provides very strict standards for the protection of personal data by establishing very detailed obligations for personal data management, providing individuals with greater rights over their personal data, and providing strict sanctions for violations.

Meanwhile, the CCPA, although similar to the GDPR, prioritizes the rights of consumers in California and is not as comprehensive as the GDPR in terms of personal data protection. On the other hand, the Indonesian PDP Law is still in the implementation stage and has big challenges related to law enforcement and public understanding of the country's right to privacy. Despite

this, the PDP Law has led to stricter regulation in the protection of personal data, although there needs to be some improvements to be on par with international regulation such as GDPR (Barati, 2023).

Solutions and Recommendations

Improvement of Regulations and Law Enforcement

Suggestions for Improving Policies and Regulations Regarding Personal Data Protection in Indonesia. To improve the protection of personal data in Indonesia, the PDP Law needs to be continuously improved, especially regarding technical regulations that regulate data security and individual rights. In addition, the government must ensure that this regulation can be implemented clearly in the public and private sectors. Strengthening the supervisory system and providing authority more to supervisory institutions can increase the effectiveness of the implementation of the PDP Law. Therefore, improving the quality of regulation and implementation is the first step to overcome this problem (Siddiqui & Farooqi, 2024).

The Importance of Law Enforcement by Law Enforcement Officials Being More Firm Against Personal Data Violations

Legal enforcement against personal data violations must be more stringent, by providing more stringent sanctions for violators. Companies or institutions that violate must be subject to heavy fines or criminal penalties if they are proven to have intentionally misused personal data. In addition, the procedure for reporting data violations must be more transparent, and the public must be provided with easy access to raise complaints or concerns. Strict and fair law enforcement will provide a sense of security and ensure that personal data protection is carried out seriously (Imran, 2024).

Increasing public awareness

Strategy to Increase Public Understanding of the Importance of Personal Data Protection The government and the private sector must work together to increase public awareness of their rights regarding the protection of personal data. Socialization campaigns that focus on the importance of maintaining the privacy of personal data need to be carried out in various channels, including social media, seminars and formal education. With a better understanding, the public will be more careful in sharing their personal data and can control its use better. The Role of Education and Media in Increasing Public Awareness Education including the protection of personal data must be included in the basic education curriculum to higher education. In addition, social media and digital platforms can be used to spread relevant information regarding how to protect personal data in cyberspace. This will help the public better understand Meireika's rights and how to effectively protect Meireika's personal information.

Strengthening Supervisory Institutions

Recommendations to Strengthen Supervisory Institutions in Maintaining Security and Protection of Personal Data Personal data protection supervisory institutions must be strengthened with greater resources and given wider authority to carry out audits and oversight of personal data management. Strengthening the capacity of this institution includes training, technology, and a more efficient monitoring system. A stronger supervisory institution will enable more effective law enforcement and ensure compliance with the PDP Law across all sectors (Saly et al., 2023).

CONCLUSION

Based on the normative and empirical analysis, this study arrives at three principal findings. First, Law No. 27 of 2022 establishes a comprehensive normative framework for personal data protection that aligns with international standards, particularly the GDPR, in terms of data subject rights, controller obligations, and cross-border transfer provisions. Second, however, implementation effectiveness remains critically undermined by the delayed establishment of the independent supervisory institution (the Personal Data Protection Commission), creating an enforcement vacuum during the 2022-2025 transition period. Third, empirical data demonstrate a significant gap between statutory rights provisions and public

awareness, with survey results indicating that the majority of respondents have experienced unauthorized use of their personal data without effective recourse mechanisms. These findings collectively demonstrate that the PDP Law's normative adequacy is not matched by institutional and societal readiness for its implementation. Based on the analysis, this study arrives at three principal findings. First, Law No. 27 of 2022 establishes a comprehensive normative framework aligning with international standards in terms of data subject rights and controller obligations. Second, implementation effectiveness remains critically undermined by the delayed establishment of the supervisory institution, creating an enforcement vacuum during 2022-2025. Third, empirical data demonstrate a significant gap between statutory rights and public awareness, with survey results indicating that most respondents experienced unauthorized use of personal data without effective recourse. These findings demonstrate that the PDP Law's normative adequacy is not matched by institutional and societal readiness.

Solutions to improve the implementation of the Personal Data Protection Act include refining regulations to provide clarity on the management of personal data, strengthening law enforcement through stricter sanctions, and strengthening the supervisory body for personal data management in accordance with established standards. Significant efforts are needed to raise public awareness about the importance of protecting personal data, as well as to empower educational institutions and the media in disseminating information related to privacy rights. It is hoped that Indonesia can build a stronger personal data protection system that keeps pace with advances in digital technology, while providing better protection for individuals in safeguarding their privacy rights. The success of personal data protection in Indonesia also depends on cooperation between the government, the private sector, and the public. The government needs to strengthen the capacity of existing supervisory agencies, such as the Personal Data Protection Commission, so that they can carry out their oversight and enforcement duties more effectively. The private sector, on the other hand, must commit to being more transparent in the management of personal data and ensuring that every policy implemented is in accordance with the intentions of the PDP Law. Meanwhile, the public must be more active in understanding their rights regarding personal data, as well as being aware of the potential risks that could occur due to their ignorance regarding ways to protect their personal data in the digital world. With synergy between these three parties, personal data protection in Indonesia can run better, creating a digital climate that is safe, trustworthy, and supports a sustainable digital economic balance.

ACKNOWLEDGEMENT

This work includes acknowledgements to those who supported the preparation of this article, particularly to the authors' home institutions and all colleagues who provided substantial input, administrative support, and assistance with relevant sources/references. The authors also express their appreciation to those who contributed to providing access to literature and/or the initial manuscript review process, enabling the article to be more comprehensive.

AUTHOR CONTRIBTUION STATEMENT

The lead author, Edi Ribut Harwanto, was responsible for the study's conception and design, data collection and analysis, drafting the manuscript, and preparing the final version. He also participated in reviewing the substance of the paper to ensure its adherence to the study framework and applicable academic regulations.

REFERENCES

Ahmad, W., Rasool, A., Javed, A. R., Baker, T., & Jalil, Z. (2022). Cyber security in IoT-based cloud computing: A comprehensive survey. *Electronics (Switzerland)*, *11*(1). https://doi.org/10.3390/electronics11010016

Alhazmi, H., Imran, A., & Alsheikh, M. A. (2024). Australasian Conference on Information Systems Perception of Digital Privacy Protection: An Empirical Study using GDPR Framework. *Australasian Conference on Information Systems (ACIS 2024)*.

Bangsu, M. N. A., Brahmanto, D. E., & Shifa, A. (2026). Legal Protection of Personal Data in Indonesia Following the Enactment of Law No. 27 of 2022 on Personal Data Protection. *Advances in Community Services Research*, *4*(2). https://doi.org/10.60079/acsr.v4i2.968

Barati, M. (2023). *Open Government Data Programs and Information Privacy Concerns : A Literature*

Review (Vol. 15, Number 1). https://doi.org/10.29379/jedem.v15i1.759

Betzing, J. H., Tietz, M., vom Brocke, J., & Becker, J. (2020). The impact of transparency on mobile privacy decision making. *Electronic Markets*, *30*(3). https://doi.org/10.1007/s12525-019-00332-3

Budiman, R. (2024). *The Development of Personal Data Protection Law in Indonesia : Challenges and Prospects for the Implementation of Law No . 27 of 2022*. (27), 24–36.

Cain, J. A., & Imre, I. (2022). Everybody wants some: Collection and control of personal information, privacy concerns, and social media use. *New Media and Society*, *24*(12). https://doi.org/10.1177/14614448211000327

Hukum, J. S., Sumarna, D., Kadriah, A., Empiris, P., & Kualitatif, P. (2023). *Penelitian Kualitatif Terhadap Hukum Empiris*. *16*(02), 101–113.

Iman, N. (2024). The fight for our personal data: analyzing the economics of data and privacy on digital platforms. In *International Journal of Law and Management* (Vol. 66, Number 6). https://doi.org/10.1108/IJLMA-12-2022-0258

Imran, A. (2024). *Perception of Digital Privacy Protection : An Empirical Study using GDPR Framework Full research paper Perception of Digital Privacy Protection*. 1–13.

Kreuter, F., Haas, G. C., Keusch, F., Bähr, S., & Trappmann, M. (2020). Collecting Survey and Smartphone Sensor Data With an App: Opportunities and Challenges Around Privacy and Informed Consent. *Social Science Computer Review*, *38*(5). https://doi.org/10.1177/0894439318816389

Mada, U. G. (2024). *Perlindungan Hukum Terhadap Data Pribadi pada Era Digital di Indonesia : Studi Undang-Undang Perlindungan Data Pribadi dan General Data Protection Regulation (GDPR)*. *6*(2), 105–124. https://doi.org/10.17933/mti.v9i1.118

Morgan, A., Sibson, R., & Jackson, D. (2022). Digital demand and digital deficit: conceptualising digital literacy and gauging proficiency among higher education students. *Journal of Higher Education Policy and Management*, *44*(3). https://doi.org/10.1080/1360080X.2022.2030275

Pathak, M., Mishra, K. N., & Singh, S. P. (2024a). Data Security and Privacy Preservation in Cloud-Based IoT Technologies: An Analysis of Risks and the Creation of Robust Countermeasures. *Recent Advances in Computer Science and Communications*, *19*(1). https://doi.org/10.2174/0126662558319054241003054922

Politou, E., Alepis, E., Virvou, M., & Patsakis, C. (2021). Privacy and Data Protection Challenges in the Distributed Era. In *Learning and Analytics in Intelligent Systems*.

Polykalas, S. E., & Prezerakos, G. N. (2019). When the mobile app is free, the product is your personal data. *Digital Policy, Regulation and Governance* , *21*(2). https://doi.org/10.1108/DPRG-11-2018-0068

Putri, A. G., Permata, D., & Asri, B. (2025). *Jurnal Cakrawala Hukum Legal Protection for Victims of Personal Data Misuse by BPJS Kesehatan Under Law Number 27 of 2022*. *16*(27), 224–238. https://doi.org/10.26905/idjch.v16i3.16492.Volume

Quach, S., Thaichon, P., Martin, K. D., Weaven, S., & Palmatier, R. W. (2022). Digital technologies: tensions in privacy and data. *Journal of the Academy of Marketing Science*, *50*(6). https://doi.org/10.1007/s11747-022-00845-y

Renuka, O., RadhaKrishnan, N., Priya, B. S., Jhansy, A., & Ezekiel, S. (2024). Data Privacy and Protection: Legal and Ethical Challenges. In *Emerging Threats and Countermeasures in Cybersecurity*. https://doi.org/10.1002/9781394230600.ch19

Romansky, R. P., & Noninska, I. S. (2020). Challenges of the digital age for privacy and personal data protection. *Mathematical Biosciences and Engineering*, *17*(5). https://doi.org/10.3934/MBE.2020286

Saly, Jeane Neltje, et al. "Analisis perlindungan data pribadi terkait uu no. 27 tahun 2022." *Jurnal Serina Sosial Humaniora* 1.3 (2023): 145-153.

Siddiqui, S. Y., & Farooqi, S. (2024). *Human Rights for the Digital Age : A Comprehensive Review*.