p–ISSN: 2723 – 6609 e-ISSN: 2745-5254
Vol. 5, No. 12, December 2024 http://jist.publikasiindonesia.id/

Implementation and Challenges of the Personal Data Protection Law in Indonesia

Fachrul Razi[1*], Hadi tuasikal[2], Dwi Pratiwi Markus[3]
Universitas Muhammadiyah Sorong, Indonesia
Email: fachrulrazy15@gmail.com[1*], hadilessytuasikal@gmail.com[2], dwypratiwimarkus@gmail.com[3]

*Correspondence

Keywords: personal data protection, law no. 27 of 2022, data leaks, data regulation, cyber security.

ABSTRACT

Law No. 27 of 2022 concerning Personal Data Protection (PDP) is a significant step in protecting the privacy and personal data of the Indonesian people. This study aims to analyze the background of the passage of this law, the content of its regulations, implementation challenges, and data leakage case studies, as well as compare these regulations with international policies. With a qualitative approach, this study uses literature studies, document analysis, and data leakage case studies such as the Tokopedia case. The results show that although the PDP Law includes basic principles of data protection, data subject rights, and data controller obligations, there are implementation challenges, such as delays in the establishment of the Personal Data Protection Agency and limitations in technological infrastructure. Comparisons with GDPR and CCPA show that the PDP Law has room for improvement in firmness and sanctions. In conclusion, while the PDP Law is a good first step, additional steps are needed, such as institutional strengthening and inter-agency coordination, to improve the effectiveness of personal data protection in Indonesia.

Introduction

Personal data protection is an important issue in today's digital era. With the rapid development of information and communication technology, the amount of personal data collected and processed by various entities, both public and private, is getting larger (Sulistianingsih, Ihwan, Setiawan, & Prabowo, 2023). Personal data, such as identity, contact, and financial information, is now a valuable asset that is often used for a variety of purposes, from marketing to business analytics. However, the increased use of personal data also carries a significant risk of data leakage (Suvil, Firdaus, Ramadhan, Putra, & Lestarika, 2024).

In Indonesia, the need for personal data protection regulations is becoming increasingly urgent as data leakage incidents increase (Sautunnida, 2018). One striking

example is the data leak that occurred on the e-commerce platform Tokopedia, where the personal information of more than 91 million user accounts was leaked to the public in 2020. The incident highlights the shortcomings in data protection and emphasizes the importance of having a strong legal framework in place to protect citizens' data (Suryanto & Riyanto, 2024).

To overcome this problem, the Indonesian government passed Law No. 27 of 2022 concerning Personal Data Protection (PDP Law). This law aims to provide better protection for personal data and establish clear obligations for data managers. Through this regulation, it is hoped that there will be an improvement in data security and individual rights related to the management of their data (Annan, 2024).

Method

This study uses a qualitative approach to analyze Law No. 27 of 2022 concerning Personal Data Protection (PDP Law) in Indonesia. This approach was chosen to allow for an in-depth exploration of the legal and practical aspects of personal data protection. The methods used in this study include:

Literature Studies

This research began with a review of the literature related to the PDP Law and personal data protection. The sources used include official documents, academic publications, legal articles, and research reports related to personal data protection. This literature study aims to gain an in-depth understanding of the legal background, basic principles, and obligations of data managers according to the PDP Law.

Document Analysis

Legal documents such as Law No. 27 of 2022 and its implementing regulations are analyzed to understand the content and legal provisions regulated in the Law. The analysis of this document includes a comparison between the PDP Law and data protection regulations in other countries to assess the strengths and weaknesses of the PDP Law.

Case Studies

This research also involves case studies of data leaks that occurred in Indonesia, such as the cases of Tokopedia and BPJS Kesehatan. This case study was carried out to understand the causes and impacts of data leaks and to assess the effectiveness of the PDP Law in dealing with the problem. Case data is obtained from news reports, analysis articles, and related official documents.

Data Analysis

Data obtained from literature studies, document analysis, and case studies were analyzed qualitatively to identify the main themes and emerging patterns related to personal data protection. This analysis aims to produce evidence-based recommendations regarding improving personal data protection in Indonesia.

Results and Discussion

Background of the Ratification of Law No. 27 of 2022

Personal data protection in Indonesia is becoming increasingly urgent in line with the rapid development of information technology and the increase in data use by various digital platforms (Hasan et al., 2024). One of the significant incidents that highlighted the need for personal data protection regulations was the leak of Tokopedia user data in 2020, which involved around 91 million user accounts. This leak revealed a huge gap in the data security system that existed at the time. This kind of incident shows how important it is to have a law that can provide clear legal protection for citizens' data (Rustam, Ardiansyah, & Saudi, 2024).

Law No. 27 of 2022 concerning Personal Data Protection was promulgated in response to the urgent need for regulations governing the management and protection of personal data. The law's legislation process involves debate and contributions from various parties, including the government, academics, and civil society, to ensure that the law comprehensively and comprehensively covers various aspects of data protection.

Analysis of the Content of Law No. 27 of 2022

1. Basic principles

Law No. 27 of 2022 concerning Personal Data Protection establishes the basic principles that must be followed in the management of personal data. These principles include:

a. Compliance: Data management must comply with applicable laws and be lawfully conducted.
b. Transparency: Data management should be done with transparency so that data subjects can understand how their data is used and stored.
c. Consistency: Data should be accurate, complete, and consistent.
d. Obligations: Data controllers are required to have a basis for data processing and to verify data regularly.
e. Disclosure: Data controllers are obliged to inform data subjects about the processing of data and grant data subjects the right to request access, update or delete their data.
f. Accountability: Data controllers must be accountable for the data they manage and be able to explain the use of that data.
g. Security: Data controllers are obliged to maintain data security by using adequate technology to protect data from leakage or misuse.
h. Limitations: Data controllers should only collect and use data that is necessary for clear and legitimate purposes.

2. Rights of data subjects

Data Subject Rights according to Law No. 27 of 2022 concerning Personal Data Protection provides a wide range of rights to data subjects, including:

a. Right of Access: Data subjects have the right to know what type of data is collected and how it is used.
b. Right to Rectification and Erasure: The data subject has the right to rectify or delete personal data that is inaccurate or irrelevant.

c. Right to Data Portability: Data subjects have the right to transfer their data to another data controller if necessary.

By providing these rights, Law No. 27 of 2022 aims to ensure that data subjects have greater control over their data and can utilize it effectively and securely.

3. Obligations of Data Managers

Law No. 27 of 2022 concerning Personal Data Protection also stipulates obligations for data managers, such as:

a. Transparency and Communication: Data managers must provide clear information regarding data processing to data subjects.
b. Data Security: Data controllers are required to implement adequate security measures to protect personal data from unauthorized access.
c. Breach Notification: The data controller must notify the data subject and the relevant authorities in the event of a data breach.

By establishing these obligations, Law No. 27 of 2022 aims to ensure that data managers are responsible for maintaining the security and transparency of personal data, as well as providing adequate protection to data subjects in the event of a breach.

Challenges in the Implementation of Law No. 27 of 2022

Challenges in the implementation of Law No. 27 of 2022 concerning Personal Data Protection include the delay in the establishment of the Personal Data Protection Agency. The delay in the establishment of the Personal Data Protection Agency (BPDP) may affect the effectiveness of supervision and enforcement of regulations related to personal data protection. Without BPDP functioning effectively, supervision of data manager compliance is not optimal. This has the potential to result in weaknesses in cracking down on breaches, as well as reducing public trust in the data protection system. This delay can also cause uncertainty for data managers in carrying out their obligations, thus increasing the risk of personal data breaches. BPDP is expected to be formed soon to ensure that Law No. 27 of 2022 can be implemented consistently and effectively, as well as provide maximum protection for personal data subjects in Indonesia (Juliana, Liza, Fatimahtuzzahra, & Imel, 2023).

Technical and institutional obstacles are also a challenge for the implementation of Law No. 27 of 2022. Technical obstacles such as lack of adequate technological infrastructure and limited human resource capacity in managing and protecting personal data. Coordination between institutions also needs to be improved to ensure effective data protection to reduce institutional constraints. Coordination between institutions also needs to be improved to ensure effective data protection. Integration and synergy between various institutions related to data protection are essential to face the complex challenges of personal data protection.

Case Study of Data Leakage in Indonesia

a. The Case of Tokopedia

The Tokopedia data leak case in 2020 is one of the prominent examples in Indonesia. The personal data of about 91 million accounts was leaked, showing weaknesses in existing data security systems. This incident highlights various problems

in the management of personal data, including the weak protection mechanisms implemented by companies. Such a large data leak not only shows potential financial losses for users but also a serious impact on individual privacy, including the risk of misuse of personal information by irresponsible parties.

This case triggered a push to strengthen personal data protection regulations in Indonesia. In this context, Law No. 27 of 2022 concerning Personal Data Protection is expected to provide a clearer and stricter legal framework for managing and protecting personal data. This regulation is expected to not only protect individuals' rights to their data but also emphasize the responsibility of data controllers in implementing adequate security measures to prevent future leaks. The experience of the Tokopedia case shows the urgency in the implementation of this law and the need for more effective supervision to prevent similar incidents.

b. Hatches and causes

The main cause of data leaks in the Tokopedia case is significant weaknesses in the data security system implemented by digital platforms and shortcomings in effective supervision. Weak data security, often the result of a lack of adequate encryption and protection, allows unauthorized parties to access and extract sensitive information. Additionally, irregularities in security system oversight and auditing contribute to delays in detecting and responding to data leaks.

The impact of these leaks is wide-ranging, including a high risk of identity misuse and privacy breaches. Affected individuals could face the risk of identity theft, fraud, and significant financial loss. On the other hand, the general public is experiencing a decline in trust in existing digital platforms and data protection systems, which can affect the adoption of the technology and overall online interactions.

International Comparison

A comparison of Law No. 27 of 2022 with data protection regulations in other countries shows significant differences in the scope and accuracy of personal data protection. The GDPR (General Data Protection Regulation) in the European Union establishes the rights of data subjects which include the rights to access, rectification, erasure, and portability of data. Data controllers under the GDPR are required to ensure transparency, and security, and provide notification in the event of a data breach. The GDPR also establishes very strict sanctions, including significant fines and severe criminal penalties for violations.

In the United States, the CCPA (California Consumer Privacy Act) grants similar rights to data subjects, such as the right to access, rectification, deletion, and data portability. The data custodian's obligations under the CCPA also include data transparency and security. Sanctions under the CCPA include significant fines as well as severe criminal penalties, similar to GDPR.

Law No. 27 of 2022 concerning Personal Data Protection in Indonesia regulates the equal rights of data subjects, including the rights to access, correct, delete, and portability of data. Data custodian's obligations include transparency, data security, and breach notification. However, the sanctions regulated in this law focus more on administrative

fines and criminal penalties, compared to large fines and severe criminal penalties implemented in the GDPR and CCPA.

Overall, although the three regulations have the same goal of protecting personal data, the GDPR and CCPA tend to be stricter and more comprehensive in their implementation and sanctions than Law No. 27 of 2022.

Conclusion

Law No. 27 of 2022 concerning Personal Data Protection is a significant step in improving personal data protection in Indonesia. However, its implementation faces various challenges, including delays in the establishment of the Personal Data Protection Agency (BPDP) and technical and institutional constraints. Case studies of data leaks, such as those on Tokopedia, show the need for stricter regulation and effective supervision. Comparisons with international regulations indicate that while Law No. 27 of 2022 already includes important rights and obligations, there is room for improvement in terms of rigor and sanctions.

Additional steps that need to be taken to improve personal data protection in Indonesia are as follows:

a. Establishment and Strengthening of BPDP
b. Technological Infrastructure Improvement
c. Education and Training
d. Strict Oversight and Enforcement: Enhance oversight of data controllers' compliance and ensure consistent enforcement of violations. This includes strengthening the mechanism for reporting violations and increasing transparency in the law enforcement process.
e. Additional Policies and Regulations: Review and adapt stricter policies and regulations to align with international standards, such as GDPR, to ensure more comprehensive and effective protection of personal data.
f. Inter-Agency Coordination: Improve coordination between various government agencies, the private sector, and civil society organizations to ensure synergy in personal data protection and overcome existing institutional constraints.

With these additional measures, it is hoped that personal data protection in Indonesia can be significantly improved, provide better security for citizens' personal data, and increase public trust in the data protection system.

Bibliography

Annan, Alaikha. (2024). Tinjauan Yuridis Perlindungan Data Pribadi Pada Sektor Kesehatan Berdasarkan Undang-Undang No. 27 Tahun 2022. *Synergy: Jurnal Ilmiah Multidisiplin*, *1*(04), 247–254.

Hasan, Zainudin, Putri, Salsabila Tiara, Gustina, Sri, Satria, Ahmad Rifki, Ramadhani, Kevin Oksandy, & Satrio, Muhammad. (2024). Tanggung Jawab Hukum Dan Ekonomi Dalam Perlindungan Data Pribadi Di Era Digital. *Causa: Jurnal Hukum Dan Kewarganegaraan*, *7*(12), 31–40.

Juliana, Siti Arbaina, Liza, Trisna, Fatimahtuzzahra, Fatimahtuzzahra, & Imel, Muhammad Akbar Hilmi. (2023). Tantangan Sosial Di Era Digital Pada Interaksi Manusia. *Significant: Journal Of Research And Multidisciplinary*, *2*(02), 245–261.

Rustam, Rustam, Ardiansyah, Irfan, & Saudi, Ahmad. (2024). DAMPAK HUKUM SIBER TERHADAP PRIVASI DATA PRIBADI DI INDONESIA. *Causa: Jurnal Hukum Dan Kewarganegaraan*, *6*(12), 31–40.

Sautunnida, Lia. (2018). Urgensi Undang-Undang Perlindungan Data Pribadi di Indonesia: Studi Perbandingan Hukum Inggris dan Malaysia. *Kanun Jurnal Ilmu Hukum*, *20*(2), 369–384.

Sulistianingsih, Dewi, Ihwan, Miftakhul, Setiawan, Andry, & Prabowo, Muchammad Shidqon. (2023). Tata kelola perlindungan data pribadi di era metaverse (telaah yuridis undang-undang perlindungan data pribadi). *Masalah-Masalah Hukum*, *52*(1), 97–106.

Suryanto, Dasep, & Riyanto, Slamet. (2024). Implementasi Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi dalam Industri Ritel Tinjauan terhadap Kepatuhan dan Dampaknya pada Konsumen. *VERITAS*, *10*(1), 121–135.

Suvil, Aulia Alayna, Firdaus, Firdaus, Ramadhan, M. Arif, Putra, Wanda Darma, & Lestarika, Dwi Putri. (2024). Implementasi Perlindungan Data Pribadi Berdasarkan Undang-Undang Nomor 11 Tahun 2020. *Jurnal Hukum, Politik Dan Ilmu Sosial*, *3*(4), 70–80.