West Science Law and Human Rights
Vol. 2, No. 04, October 2024, pp. 421~428

Normative Study of Law No. 27 of 2022 on the Protection of Personal Data and its Impact on the Fintech Industry in Indonesia

Zulkham Sadat Zuwanda[1], Loso Judijanto[2], Hendri Khuan[3], Andri Triyantoro[4]
[1]IPDN
[2]IPOSS Jakarta
[3]Universitas Borobudur
[4]LBH DPNI

Article Info

Article history:

Received October, 2024
Revised October, 2024
Accepted October, 2024

Keywords:

Personal Data Protection
Fintech Industry
Data Security
Regulatory Compliance
Indonesia

ABSTRACT

The enactment of Law No. 27 of 2022 on Personal Data Protection marks a pivotal moment in Indonesia's regulatory framework, particularly for industries that handle significant amounts of personal data, such as the financial technology (fintech) sector. This study provides a normative juridical analysis of the PDP Law and examines its impact on the fintech industry. The research focuses on the law's key provisions, including consent requirements, data breach notification, and data security obligations. Additionally, the study explores the operational challenges fintech companies face in complying with the law, such as the costs of compliance, technical requirements, and the need for employee training. While the PDP Law enhances consumer trust by offering greater protection and transparency, it also presents hurdles that fintech firms must overcome to ensure compliance. The analysis concludes with recommendations for fintech companies to balance legal obligations with innovation to maintain competitiveness in Indonesia's evolving digital economy.

Corresponding Author:

Name: Zulkham Sadat Zuwanda
Institution Address: IPDN
e-mail: szuwanda@gmail.com

1. INTRODUCTION

The rapid growth of digital technology in Indonesia has significantly transformed the financial technology (fintech) industry through innovations like digital payments, peer-to-peer lending, and online investment platforms. This shift has boosted financial inclusion, especially for underserved populations, by improving access to efficient and affordable digital solutions [1]. Fintech has also contributed to economic growth by optimizing financial services and promoting financial independence [2]. Moreover, fintech has reshaped the financial landscape by enabling electronic transactions and reducing reliance on conventional payment methods [3]. However, challenges such as security risks and data privacy concerns persist, as digital transactions increase vulnerability to fraud and cyber threats [1]. The Financial Services Authority (OJK) faces difficulties in supervising fintech-related crimes, emphasizing the need for stronger regulatory frameworks Fintech, the threat of technology in the conventional financial system [4]. Current regulations, such as Bank Indonesia Regulation No. 19/12/PBI/2017 and Financial

Services Authority Regulation No. 77/POJK.01/2016, aim to protect consumers and ensure fairness in fintech [5], but further legal reforms are needed to stabilize the sector [2].

The enactment of Indonesia's Law No. 27 of 2022 on Personal Data Protection (PDP Law) marks a significant advancement in safeguarding personal data, especially in data-intensive sectors like fintech. This law introduces comprehensive regulations for the collection, storage, processing, and dissemination of personal data, enhancing individual control and imposing stringent compliance requirements on businesses. The PDP Law addresses vulnerabilities related to data breaches and misuse, which are common in fintech and banking, by establishing a robust legal framework for data protection. Key aspects include a unified legal framework consolidating fragmented regulations, with specific guidelines for sectors like fintech and banking [6], and the recommendation to establish a Personal Data Protection Commission (PDPC) for oversight [7]. The law empowers consumers by granting rights to access, correct, and delete personal data [6] and aims to address mobile banking risks and cyber threats to enhance customer data security [8], [9]. However, challenges remain, including low public awareness and digital literacy, which may hinder effective implementation [10], and the need for improved infrastructure and resources to support enforcement [10].

The implementation of the Personal Data Protection (PDP) Law presents both opportunities and challenges for the fintech industry, which depends on personal data to provide innovative services. Fintech companies must now navigate legal obligations such as obtaining explicit user consent, ensuring data security, and reporting data breaches, which affect their operations and strategies. These obligations complicate onboarding and data management [7] and require robust cybersecurity to prevent threats like phishing and ransomware [11]. While the PDP Law increases operational costs by mandating breach reporting [11], it also opens opportunities through Regulatory Technology (RegTech), streamlining compliance and improving risk management [12]. Advanced technologies like AI and blockchain further enhance security and efficiency [13], but the evolving regulatory landscape demands rapid adaptation and collaboration between regulators and industry stakeholders to support innovation while maintaining financial stability [13], [14].

This paper aims to provide a normative juridical analysis of Law No. 27 of 2022 and its impact on the fintech industry in Indonesia. By examining the key provisions of the PDP Law and analyzing its implications for fintech businesses, this study will explore the legal challenges that fintech companies face in adhering to the law's requirements. Furthermore, the paper will evaluate how the PDP Law may influence the future development of the fintech sector in Indonesia, particularly in terms of data governance, consumer trust, and regulatory compliance.

The objectives of this paper are threefold. First, to provide a comprehensive overview of Law No. 27 of 2022 on Personal Data Protection, focusing on its core legal principles and provisions. Second, to analyze the specific impact of the law on the fintech industry, identifying key areas where fintech companies will need to adjust their operations to comply with the new regulations. Lastly, the paper will discuss the potential legal risks and opportunities that arise from the implementation of the PDP Law and provide recommendations for fintech companies to achieve compliance while maintaining competitiveness in the digital financial services market.

2. LITERATURE REVIEW

2.1 Importance of Personal Data Protection in the Digital Age

The digital economy's reliance on personal data has amplified privacy and security concerns, necessitating robust data protection measures. Westin's concept of "privacy as control" highlights the importance

of individuals having authority over their personal data, a principle echoed in modern regulations. The Ponemon Institute's findings on the rising frequency and cost of data breaches underscore the urgent need for businesses to implement effective data protection strategies, especially in industries like finance and healthcare, where the stakes are particularly high. Data Loss Prevention (DLP) solutions play a crucial role in safeguarding sensitive information while maintaining user privacy, though aligning DLP with privacy principles presents challenges [15]. Stricter regulations, such as the GDPR, are essential for protecting personal data, with global collaboration necessary to combat cross-border cybercrime, alongside public awareness efforts [16]. India's Digital Personal Data Protection Act, 2023, reflects regulatory efforts to tackle data privacy challenges and protect sensitive information [17]. Techniques like encryption, access control, and anonymization are vital for data privacy, yet evolving cyber threats and regulatory compliance remain challenging [18]. Balancing innovation and privacy requires thoughtful regulation to ensure technological advancements do not compromise personal security [19].

2.2 Global Legal Frameworks for Personal Data Protection

The General Data Protection Regulation (GDPR) has significantly influenced global data protection laws, setting a high standard for privacy and data security. Its principles, such as "privacy by design," have been adopted by various jurisdictions, including Indonesia and California, to enhance personal data protection. The GDPR's framework, which emphasizes individual rights, transparency, and accountability, serves as a model for other countries developing their own legal frameworks in response to the demands of the digital economy. Indonesia's Personal Data Protection Law aims to emulate the GDPR's approach, although the country faces challenges in implementation and enforcement [20]. In the U.S., the California Consumer Privacy Act (CCPA) reflects GDPR principles by granting individuals control over their personal data, but the lack of a unified federal privacy law results in a fragmented regulatory landscape [21]. Both GDPR and CCPA emphasize individual rights, like data portability and the "right to be forgotten," though the U.S. approach is more sector-specific [21]. GDPR imposes significant fines for non-compliance, while U.S. penalties vary by state [21]. Global issues like cybercrime and data misuse necessitate strict regulations and international collaboration [16], and the GDPR's approach to defining personal data and anonymization provides a clear framework for assessing data protection risks [22], [23].

2.3 Legal Framework for Personal Data Protection in Indonesia

Indonesia's digital economy has rapidly expanded, necessitating robust legal frameworks to protect personal data, particularly in sectors like fintech and banking. The enactment of Law No. 27 of 2022 on Personal Data Protection (PDP Law) represents a significant advancement, aligning with international standards like the GDPR. It addresses previous regulatory gaps by defining clear rights and obligations regarding personal data, requiring explicit consent for processing, implementing security measures, and mandating breach reporting, with penalties for non-compliance to incentivize better practices. This is crucial for fintech, where personal data is integral to services like digital payments and credit scoring. Data controllers must now obtain explicit consent, ensuring transparency and user control [7], and organizations are required to implement strong security measures to minimize breaches [9]. The law mandates breach reporting to authorities, promoting accountability [8], while administrative sanctions and fines enforce compliance [7]. For fintech, this law mitigates risks related to data misuse, which can lead to financial losses [7], and in banking, it enhances public trust by safeguarding customer data amidst increasing cyber threats [8].

2.4 Impact of Data Protection Laws on the Fintech Industry

The introduction of comprehensive data protection laws, such as the Personal Data Protection (PDP) Law, presents both opportunities and challenges for fintech companies in Indonesia. These laws can enhance consumer trust, crucial for the growth of digital financial services, as compliance can lead to increased customer retention and market share. Consumers are more likely to engage with businesses that prioritize data protection, with a PwC study showing that 85% of consumers would avoid businesses with poor data protection practices [7]. Adhering to these regulations allows fintech companies to expand their market share by fostering customer loyalty, as trust is a key factor in consumer decision-making [1]. However, implementation requires significant operational adjustments, including investments in data protection technologies and employee training [7]. Smaller fintech firms may struggle with resource constraints, creating operational challenges in meeting the law's requirements [2]. Non-compliance poses financial risks, as companies can face substantial fines and reputational damage, such as fines up to 4% of global annual revenue under GDPR for serious breaches [8], [24].

3. METHODS

3.1 Research Design

This research adopts a qualitative approach with a normative juridical design. The primary focus is on interpreting and analyzing legal norms, statutory provisions, and regulatory frameworks as they apply to the fintech sector in Indonesia. A normative juridical design is appropriate for this study because it allows for a detailed examination of the legal texts related to personal data protection, as well as their implications for businesses operating in data-driven industries like fintech.

The study does not involve empirical data from the field but rather focuses on analyzing existing legal materials, such as statutes, government regulations, academic literature, and case law. Additionally, the research looks into the practical application of the law and its legal impact on the operations of fintech companies.

3.2 Data Collection Methods

The data collection process for this study involves gathering two main types of materials: primary and secondary legal materials. Primary legal materials, including statutory texts and regulations, serve as the foundational sources of law. These materials include Law No. 27 of 2022 on Personal Data Protection (PDP Law), which is the central focus of the analysis, examining data protection principles, obligations, sanctions, and enforcement mechanisms. Additionally, the Electronic Information and Transactions Law (Law No. 11 of 2008) is reviewed for its historical context, along with other relevant regulations related to cybersecurity and electronic systems. Secondary legal materials provide interpretations and analyses that offer context and practical insights. These include academic journals, books on fintech regulation, reports from regulatory authorities like the Ministry of Communication and Informatics and the Financial Services Authority (OJK), as well as industry reports from fintech associations and legal commentaries. Case law and expert commentary are also analyzed to understand the practical challenges of compliance and the impact of the PDP Law on the fintech industry.

3.3 Data Analysis

The data analysis process involves interpreting both primary and secondary legal materials to assess the impact of Law No. 27 of 2022 on the fintech industry. A systematic approach will be applied to identify relevant legal provisions, explore their practical implications, and examine their enforcement within the fintech sector. The analysis is structured into three main components: first, a legal interpretation will be conducted to examine key provisions of the PDP Law, including consent, data processing obligations, breach notifications, and sanctions, with a focus on their applicability

to fintech companies that heavily rely on customer data. Second, a juridical analysis will assess the regulatory implications, examining how the law shapes fintech companies' responsibilities and interacts with other regulations, such as the Electronic Information and Transactions Law and Financial Services Authority (OJK) sectoral regulations, while evaluating potential legal risks and mitigation strategies. Finally, an impact evaluation will explore the operational challenges fintech companies may face in complying with the law, including implementation costs and reputational risks, as well as the opportunities for building consumer trust and enhancing competitiveness in the digital financial services market.

4. RESULTS AND DISCUSSION

4.1 Compliance Obligations under the PDP Law for Fintech Companies

One of the key findings of this study is that Law No. 27 of 2022 imposes several new compliance obligations on fintech companies operating in Indonesia. These obligations are aligned with international data protection standards, particularly the European Union's General Data Protection Regulation (GDPR). The PDP Law mandates that all companies, including fintech firms, comply with the following core requirements:

A major focus of the PDP Law is ensuring that fintech companies obtain explicit and informed consent from users before collecting or processing their data. Under Article 20 of the law, fintech companies must ensure that individuals are made aware of how their data will be used, the purpose of the data collection, and the duration for which the data will be retained. This provision significantly impacts fintech firms, which often rely on large datasets to deliver personalized financial services, such as credit scoring, digital payments, and investment advice.

Failure to obtain explicit consent may lead to legal penalties and reputational damage. The law's emphasis on transparency means that fintech companies must revise their privacy policies to provide detailed information to users. In practice, this requires businesses to re-engineer their data collection processes and invest in systems that ensure user consent is recorded and managed effectively.

The PDP Law introduces stringent obligations for fintech companies in the event of a data breach. Under Article 46, fintech firms must notify the relevant regulatory authority and affected individuals within three days of discovering a data breach. This provision creates operational challenges for fintech companies, particularly those with limited resources to monitor and respond to data breaches in real-time.

The rapid notification requirement has significant implications for fintech firms that handle large amounts of sensitive financial data. A failure to report data breaches within the required timeframe can result in significant fines and legal liabilities. Furthermore, data breaches may lead to long-term damage to customer trust and loyalty, which are critical to the success of fintech businesses.

4.2 Operational Challenges for Fintech Companies

While the PDP Law enhances consumer protection, it also presents several operational challenges for fintech companies. These challenges relate to the cost of compliance, the technical requirements for data security, and the need for staff training and capacity building. Compliance with the PDP Law requires fintech companies to implement robust data protection measures, which can be costly, particularly for small and medium-sized fintech firms. Companies must invest in technologies that ensure data security, such as encryption and secure storage systems, as well as systems that manage consent and enable real-time reporting of data breaches.

In addition, the need to hire data protection officers (DPOs) and provide ongoing staff training represents an additional financial burden. The cost of ensuring compliance may be particularly

prohibitive for fintech startups, which often operate with limited resources. As a result, smaller fintech companies may struggle to compete with larger, more established firms that have greater capacity to absorb compliance costs. The PDP Law introduces several technical and organizational requirements for fintech companies, which must implement appropriate security measures to protect personal data. Article 35 of the law requires businesses to use encryption, pseudonymization, and other data protection techniques to prevent unauthorized access to personal data. Additionally, fintech companies must ensure that personal data is processed and stored in secure environments.

These requirements necessitate the adoption of advanced technologies, which may require significant investment. Furthermore, fintech companies must establish internal data protection policies and procedures to ensure compliance with the law. This includes conducting regular risk assessments, implementing incident response plans, and establishing clear lines of responsibility for data protection. To comply with the PDP Law, fintech companies must ensure that their employees are adequately trained in data protection practices. This is particularly important for employees who handle personal data or are responsible for customer interactions. Training programs must focus on raising awareness about the importance of data protection, the legal requirements for processing personal data, and the steps to take in the event of a data breach. Moreover, fintech companies must appoint data protection officers (DPOs) to oversee compliance with the PDP Law. DPOs play a critical role in ensuring that companies adhere to the law's requirements and respond to any data protection issues that may arise. However, the appointment of DPOs represents an additional cost for fintech firms, particularly those with limited financial and human resources.

4.3 Impact on Consumer Trust and Market Competitiveness

The implementation of Law No. 27 of 2022 presents both challenges and opportunities for fintech companies in Indonesia. On one hand, compliance with the PDP Law requires significant investment in data protection measures, which may strain the resources of fintech companies, particularly smaller firms. On the other hand, adherence to the law can enhance consumer trust and improve the competitiveness of fintech companies in the long term. Compliance with the PDP Law has the potential to enhance consumer trust in fintech services. The law provides consumers with greater control over their personal data, which can lead to increased confidence in fintech platforms. According to a PwC (2020) report, 85% of consumers are unwilling to engage with businesses if they have concerns about how their data is handled. Therefore, by complying with the PDP Law, fintech companies can reassure consumers that their data is being handled securely and in accordance with the law.

Moreover, by implementing best practices for data protection, fintech companies can differentiate themselves from competitors that may not prioritize consumer privacy. This could lead to increased customer loyalty and a larger market share, as consumers increasingly seek out services that prioritize data protection. While the initial costs of compliance may be high, the PDP Law can ultimately contribute to the competitiveness of fintech companies. Firms that comply with the law may be better positioned to expand their operations both domestically and internationally, particularly in markets that have stringent data protection regulations. By demonstrating compliance with international data protection standards, fintech companies can attract new customers and investors, thereby enhancing their long-term growth potential. Furthermore, companies that prioritize data protection may be able to form partnerships with other businesses and institutions that require strict data protection standards. For example, banks, insurance companies, and other financial institutions may prefer to collaborate

with fintech companies that demonstrate a strong commitment to data security and compliance.

4.4 Juridical Implications and Recommendations

The normative juridical analysis of Law No. 27 of 2022 reveals that while the law provides a solid framework for protecting personal data in Indonesia, there are several areas where fintech companies may face challenges in implementation. The rapid pace of technological change in the fintech sector necessitates continuous updates to the regulatory framework to ensure that it remains relevant and effective.

One of the key juridical challenges for fintech companies is the interpretation of the law's provisions regarding cross-border data transfers. Fintech companies often operate across multiple jurisdictions, and the PDP Law imposes restrictions on the transfer of personal data to countries that do not have equivalent data protection standards. This creates legal uncertainties for fintech firms that rely on global data processing systems.

Moreover, the enforcement of the PDP Law remains a critical issue. While the law establishes penalties for non-compliance, there are concerns about the capacity of Indonesian regulators to effectively monitor and enforce compliance, particularly in an industry as dynamic as fintech.

Recommendations for Fintech Companies

To navigate the challenges posed by the PDP Law, fintech companies should adopt the following strategies:

a. Companies should invest in state-of-the-art data protection technologies, such as encryption and secure cloud storage, to ensure compliance with the law's security requirements.
b. Fintech companies should appoint data protection officers to oversee compliance efforts and ensure that data protection policies are implemented effectively.
c. Companies must provide regular training for employees to ensure that they are aware of their responsibilities under the PDP Law and can respond appropriately to data protection issues.
d. Fintech firms should establish comprehensive incident response plans to manage data breaches effectively and ensure that they meet the law's breach notification requirements.

5. CONCLUSION

The introduction of Law No. 27 of 2022 on Personal Data Protection represents a crucial step in protecting personal data in Indonesia, particularly for data-driven sectors like fintech. The law introduces comprehensive requirements for data processing, consent, and breach notifications, imposing strict obligations on fintech companies. While these obligations strengthen consumer trust and data security, they also present operational challenges, particularly in terms of cost, technical implementation, and employee training. Fintech companies must invest in advanced data protection technologies and develop clear internal policies to ensure compliance with the law. Despite these challenges, compliance with the PDP Law offers fintech firms the opportunity to build consumer confidence, improve competitiveness, and align with international data protection standards.

The study emphasizes that while the PDP Law is a positive development for personal data protection, further efforts are needed to address cross-border data transfer challenges and enforcement capacities. By adopting proactive strategies, fintech companies can navigate these legal challenges while continuing to innovate and grow in Indonesia's dynamic digital economy.

REFERENCES

[1] Z. Qur'anisa, M. Herawati, L. Lisvi, M. H. Putri, and O. Feriyanto, "Peran Fintech Dalam Meningkatkan Akses Keuangan di Era Digital: Studi Literatur," *GEMILANG J. Manaj. dan Akunt.*, vol. 4, no. 3, pp. 99–114, 2024.

[2] M. S. N. Azizah and A. Suryono, "Perlindungan Hukum Jasa Keuangan Fintech Dalam Perkembangan Ekonomi Di Indonesia Pada Era Indusri 4.0," in *Prosiding Seminar Nasional Ilmu Pendidikan*, 2024, pp. 212–221.
[3] R. M. Permana, "Analysis of the Financial Performance of State-Owned Enterprises (SOEs) in the Mining Sector Listed on the Indonesia Stock Exchange in 2018-2022," *Indo-Fintech Intellectuals J. Econ. Bus.*, vol. 3, no. 2, pp. 371–383, Sep. 2023, doi: 10.54373/ifijeb.v3i2.250.
[4] J. J. B. Suseno, T. F. M. Paksi, and Y. Yusriando, "Role of the Financial Service Authority of the Republic of Indonesia in Determining Financial Technology Crime as Bijzondere Toestanden," *Al-Bayyinah*, vol. 8, no. 1, pp. 76–98, 2024.
[5] B. Widagdo and C. Sa'diyah, "Business sustainability: Functions of financial behavior, technology, and knowledge," *Probl. Perspect. Manag.*, vol. 21, no. 1, pp. 120–130, 2023, doi: 10.21511/ppm.21(1).2023.11.
[6] Y. L. Ngompat and M. G. M. Maran, "Legal Development And Urgency Of Personal Data Protection In Indonesia," *JILPR J. Indones. Law Policy Rev.*, vol. 5, no. 3, pp. 627–635, 2024.
[7] A. Rohendi and D. B. Kharisma, "Personal data protection in fintech: A case study from Indonesia," *J. Infrastructure, Policy Dev.*, vol. 8, no. 7, p. 4158, 2024.
[8] M. S. Lazuardy, M. Rachmawati, T. Marlina, and J. Umar, "Legal framework for protecting bank customers against personal data leakage in the digital era: A study of Indonesian regulations," *Indones. J. Multidiscip. Sci.*, vol. 3, no. 10, 2024.
[9] B. G. A. Rama and I. P. E. Rusmana, "Legal protection of personal data of banking customers in Indonesia: Human rights perspective," *J. Law Sci.*, vol. 6, no. 3, pp. 367–375, 2024.
[10] C. Sigalas, "Competitive advantage: the known unknown concept," *Manag. Decis.*, vol. 53, no. 9, pp. 2004–2016, Oct. 2015, doi: 10.1108/MD-05-2015-0185.
[11] O. P. Olaiya, T. O. Adesoga, A. Ojo, O. D. Olagunju, O. O. Ajayi, and Y. O. Adebayo, "Cybersecurity strategies in fintech: safeguarding financial data and assets," *GSC Adv. Res. Rev.*, vol. 20, no. 1, pp. 50–56, 2024.
[12] B. E. Abikoye, S. C. Umeorah, A. O. Adelaja, O. Ayodele, and Y. M. Ogunsuji, "Regulatory compliance and efficiency in financial technologies: Challenges and innovations," *World J. Adv. Res. Rev.*, vol. 23, no. 1, pp. 1830–1844, 2024.
[13] S. Obeng, T. V. Iyelolu, A. A. Akinsulire, and C. Idemudia, "The Transformative Impact of Financial Technology (FinTech) on Regulatory Compliance in the Banking Sector," *World J. Adv. Res. Rev.*, vol. 23, no. 1, pp. 2008–2018, 2024.
[14] C. Kurniawan and K. Nuringsih, "The Predictors of Competitive Advantage Among F&B MSMEs in Post-Pandemic Era," *Int. J. Appl. Econ. Bus.*, vol. 1, no. 1, pp. 217–223, Jul. 2023, doi: 10.24912/ijaeb.v1i1.217-223.
[15] N. A. Zaini and M. F. Zolkipli, "A Survey on Balancing Data Loss Prevention (DLP) with User Privacy in a Data-Driven World," *J. Innov. Technol.*, vol. 2024, 2024.
[16] F. A. Salsabila and A. A. IImih, "Penyalahgunaan Data Pribadi Sebagai Bentuk Kejahatan Sempurna Dalam Perspektlf Hukum Siber," *ALADALAH J. Polit. Sos. Huk. dan Hum.*, vol. 2, no. 4, pp. 176–181, 2024.
[17] B. Ehimuan, O. Chimezie, O. V. Akagha, O. Reis, and B. B. Oguejiofor, "Global data privacy laws: A critical review of technology's impact on user rights," *World J. Adv. Res. Rev.*, vol. 21, no. 2, pp. 1058–1070, 2024.
[18] O. A. Farayola, O. L. Olorunfemi, and P. O. Shoetan, "Data privacy and security in it: a review of techniques and challenges," *Comput. Sci. IT Res. J.*, vol. 5, no. 3, pp. 606–615, 2024.
[19] B. Singh, "Cherish Data Privacy and Human Rights in the Digital Age: Harmonizing Innovation and Individual Autonomy," in *Balancing Human Rights, Social Responsibility, and Digital Ethics*, IGI Global, 2024, pp. 199–226.
[20] R. Natamiharja and I. Setiawan, "Guarding Privacy in the Digital Age: A Comparative Analysis of Data Protection Strategies in Indonesia and France," *Jambe Law J.*, vol. 7, no. 1, pp. 233–251, 2024.
[21] S. S. Bakare, A. O. Adeniyi, C. U. Akpuokwe, and N. E. Eneh, "Data privacy laws and compliance: a comparative review of the EU GDPR and USA regulations," *Comput. Sci. IT Res. J.*, vol. 5, no. 3, pp. 528–543, 2024.
[22] V. Rupp and M. von Grafenstein, "Clarifying 'personal data' and the role of anonymisation in data protection law including and excluding data from the scope of the GDPR (more clearly) through refining the concept of data protection," *Comput. Law Secur. Rev.*, vol. 52, p. 105932, 2024.
[23] M. BLIKHAR, "LEGAL REGULATION OF PERSONAL DATA PROTECTION," 2024.
[24] D. Fidhayanti, M. S. Mohd Noh, R. Ramadhita, and S. Bachri, "Exploring The Legal Landscape of Islamic Fintech in Indonesia: A Comprehensive Analysis of Policies and Regulations," *F1000Research*, vol. 13, p. 21, 2024.