Jurnal Serina Sosial Humaniora
Vol. 2, No. 1, Februari 2024 hlm: 108-114 ISSN-L 2987-1506 (Versi Elektronik)

DECENTRALIZED DATA: A SOLUTION FOR COMPLIANCE WITH INDONESIA'S PERSONAL DATA PROTECTION LAW

Lewiandy[1]

[1]Fakultas Hukum, Universitas Tarumanagara, Jakarta
Email: lewiandy@fh.untar.ac.id

ABSTRACT

The Personal Data Protection Law, or UU Perlindungan Data Pribadi 2022, mandates compliance requirements for businesses in Indonesia to manage customer data. However, storing data in a single centralized database in Indonesia poses risks to data security and privacy. Decentralized technologies like blockchain can offer a solution by returning data to customers, ensuring they remain in control of their personal information. This paper aims to analyze the compliance requirements of the UU and provide a solution through decentralized technology , The UU Perlindungan Data Pribadi 2022 is the first comprehensive law in Indonesia to govern personal data protection in both electronic and non-electronic systems, covering data ownership rights, prohibitions on data use, and collection, storage, processing, and transfer of personal data. The law establishes responsibilities for the processing of personal data and rights for individuals. By leveraging decentralized technology, this paper aims to provide a comprehensive solution for businesses in Indonesia to comply with the Personal Data Protection Law while ensuring data security and privacy. The solution involves returning data to customers, ensuring they remain in control of their personal information. This approach aligns with the data-centric security approach, which is integral to various worldwide data compliance regulations and standards.

Keywords: *personal data protection law, data decentralization, personal data*

ABSTRAK

Hukum Perlindungan Data Pribadi, atau UU Perlindungan Data Pribadi 2022, mengamanatkan persyaratan kepatuhan bagi bisnis di Indonesia untuk mengelola data pelanggan. Namun, menyimpan data dalam sebuah basis data terpusat di Indonesia menimbulkan risiko terhadap keamanan dan privasi data. Teknologi terdesentralisasi seperti *blockchain* dapat menawarkan solusi dengan mengembalikan kontrol data kepada pelanggan, memastikan bahwa mereka tetap memiliki kendali atas informasi pribadi mereka. Makalah ini bertujuan untuk menganalisis persyaratan kepatuhan dari UU dan menyajikan solusi melalui teknologi terdesentralisasi. UU Perlindungan Data Pribadi 2022 merupakan undang-undang komprehensif pertama di Indonesia yang mengatur perlindungan data pribadi baik dalam sistem elektronik maupun non-elektronik, mencakup hak kepemilikan data, larangan penggunaan data, serta pengumpulan, penyimpanan, pengolahan, dan transfer data pribadi. Undang-undang ini menetapkan tanggung jawab untuk pengolahan data pribadi dan hak-hak bagi individu. Dengan memanfaatkan teknologi terdesentralisasi, makalah ini bertujuan untuk memberikan solusi komprehensif bagi bisnis di Indonesia agar patuh terhadap Undang-Undang Perlindungan Data Pribadi sambil memastikan keamanan dan privasi data. Solusi ini melibatkan pengembalian data kepada pelanggan, memastikan bahwa mereka tetap memiliki kendali atas informasi pribadi mereka. Pendekatan ini sejalan dengan pendekatan keamanan berbasis data, yang merupakan bagian integral dari berbagai regulasi dan standar kepatuhan data di seluruh dunia.

Kata Kunci: undang-undang perlindungan data pribadi, desentralisasi data, data pribadi

1. PENDAHULUAN

The advent of the digital age has ushered in an era where data has become one of the most valuable assets for individuals and organizations alike. With the exponential increase in data generation and utilization, concerns regarding data privacy and security have escalated, prompting nations worldwide to enact stringent data protection laws. Indonesia, responding to these global trends, introduced the Personal Data Protection Law (Undang-Undang Perlindungan Data Pribadi) in 2022. This law represents a significant milestone in the country's efforts to safeguard personal data, imposing comprehensive obligations on data processors and controllers to ensure data privacy and security.

 https://doi.org/10.24912/jssh.v2i1.34245

However, the traditional centralized approach to data management, predominantly employed by organizations, has shown significant limitations in adhering to these new legal requirements. Centralized systems, with their inherent risks of data breaches, limited transparency in data processing, and challenges in managing informed consent, struggle to meet the stringent standards set by the law. This misalignment not only poses compliance risks but also raises concerns about the efficacy and reliability of data management practices in the current legal framework.

In this context, decentralized data management systems, particularly those leveraging blockchain technology, emerge as a promising alternative. These systems offer inherent advantages in terms of enhanced security, transparency, and immutability, qualities that align closely with the requirements of Indonesia's Personal Data Protection Law. This research paper aims to explore the feasibility and effectiveness of decentralized systems in ensuring auto-compliance with the law. It delves into the challenges of the centralized approach, compares it with the decentralized paradigm, and proposes how the latter can address compliance issues more efficiently and reliably. Through this exploration, the paper seeks to contribute to the discourse on data management practices in the digital era, offering insights into how decentralized systems can revolutionize the way personal data is managed and protected in compliance with legal standards.

The implementation of Indonesia's Personal Data Protection Law has brought to the forefront a significant challenge for organizations: the need to adapt their data management practices to comply with stringent legal standards. Centralized data management systems, which have been the norm, are increasingly proving inadequate in meeting the law's requirements for transparency, data integrity, and secure data handling. These systems face difficulties in efficiently managing informed consent, ensuring data security, particularly in cross-border data transfers, and maintaining the accuracy and consistency of data. This gap in compliance not only exposes organizations to legal risks but also undermines public trust in how personal data is managed. Therefore, there is a pressing need to explore alternative data management solutions that can seamlessly align with the legal framework while enhancing data security and integrity. Decentralized data management systems, particularly those utilizing blockchain technology, may offer such a solution. However, the extent to which these decentralized systems can address the compliance challenges posed by the law and the practicality of their implementation in the existing digital infrastructure remains a problem that requires thorough investigation and analysis. This research paper seeks to address this gap by examining the potential of decentralized systems in ensuring compliance with Indonesia's Personal Data Protection Law and evaluating their viability as a sustainable alternative to centralized data management practices.

2. METODE PENELITIAN

The type analysis used in writing this paper is descriptive-prescriptive with normative approach. The aim of this paper is to describe the problems arises of centralized approach when faced with the challenge of the adoption of the data protection law. In this regard, the paper starts with analyzing the obligations of data processors under the Indonesian Data Protection Law. After reviewing the normative regulation requirement, we will start explaining the problems of the present centralized data processing problem and eventually analyze if the decentralized approach would be a suitable solution for for compliance. This paper analyzes the problem through normative approach which means that in seeing the problems presented, we gather data from relevant sources, both legal and non-legal, to later be analyzed based on available literature.

3. HASIL DAN PEMBAHASAN

In the intricate landscape of personal data governance as outlined by Indonesia's Personal Data Protection Law, Article 16 emerges as a pivotal element. This article delineates an extensive range of activities constituting personal data processing - from the initial stages of acquisition and collection to the nuanced tasks of analysis, storage, and the eventual destruction or deletion of data. The law imposes rigorous principles that govern these processes, including the necessity for data collection to be limited, specific, transparent, and legally sound. Furthermore, it stipulates that data processing should align with the initially stated purposes and be executed while ensuring the rights of data subjects.

A critical aspect of Article 16 is its emphasis on accuracy, completeness, and the need for data to be current and accountable. This focus addresses the risks associated with data mismanagement, particularly in contexts of unauthorized access, disclosure, alteration, or destruction. The law mandates transparent communication about the purposes and methodologies of data processing, alongside a requirement for the responsible disposal of data following its retention period or at the behest of the data subject, unless otherwise directed by legal frameworks.

The stipulations of Article 16, when viewed through the lens of decentralized data systems, underscore the potential benefits of such systems in achieving automatic compliance. Decentralized data management, with its inherent traits of transparency, immutability, and distributed control, aligns seamlessly with the law's demands for precision, accountability, and secure data handling. In essence, these systems could offer a paradigmatic shift in managing personal data, ensuring that legal compliance is embedded into the very architecture of data processing and management. This alignment not only augments the security and integrity of personal data but also enhances the efficiency and efficacy of regulatory adherence, making decentralized data systems a compelling solution in the quest for legal compliance under Indonesia's Personal Data Protection Law.

Indonesia's Personal Data Protection Law meticulously outlines the obligations of data processors, ensuring the ethical and legal handling of personal data, an aspect crucial in the era of digital information. Article 21 of the law emphasizes informed consent, mandating data controllers to transparently inform data subjects about various aspects of data processing. This includes the legality, purpose, type, retention period, and processing duration of the personal data, along with the rights of the data subjects. The article also stipulates the necessity for data controllers to promptly update data subjects about any changes to this information, ensuring ongoing transparency and accountability in data processing practices.

Furthermore, Article 22 delves into the specifics of obtaining consent. It requires that consent for data processing be explicit, either in a written or recorded format, and can be conveyed through electronic or non-electronic means. The law demands that the consent process be clear, distinguishable, accessible, and employ simple language, ensuring that the data subjects are fully aware and understanding of what they are consenting to. Importantly, any consent that does not meet these criteria is considered legally void, underscoring the law's commitment to protect data subjects’ rights and autonomy.

In a significant move to safeguard data subjects' interests, Article 23 declares any contractual clause that includes data processing requests without explicit consent from the data subject as null and void. This provision serves as a critical check against implicit or coerced consent, further fortifying the rights of data subjects in the digital realm.

 https://doi.org/10.24912/jssh.v2i1.34245

Lastly, Article 29 addresses the accuracy, completeness, and consistency of personal data. Data controllers are obligated to ensure that personal data is processed in accordance with these principles, in line with regulatory requirements. The law mandates verification processes to maintain these standards, thereby ensuring the integrity and reliability of the data being processed.

Incorporating these legal mandates into the framework of decentralized data systems highlights their potential to automatically comply with such regulations. Decentralized systems, by design, can support transparent, consent-based, and purpose-specific data processing, offering an innovative and efficient approach to managing personal data. This alignment with the law's requirements not only enhances the security and integrity of personal data but also simplifies the compliance process, making decentralized data systems a viable and effective solution in the context of Indonesia's Personal Data Protection Law.

The provisions outlined in Articles 55 and 56 of Indonesia's Personal Data Protection Law focus on the transfer of personal data, both within and outside the jurisdiction of the Republic of Indonesia. Article 55 of the Indonesian Personal Data Protection Law addresses the transfer of personal data between data controllers within the national jurisdiction. It allows for such transfer, provided that both the transferring and receiving parties adhere to the data protection measures stipulated in the law. This provision ensures that data protection is maintained throughout the process of data transfer within the country, underscoring a seamless safeguarding of personal data.

In a more global context, Article 56 extends the scope of data transfer to international boundaries. It permits the transfer of personal data to data controllers or processors outside Indonesia, subject to the conditions set forth in the law. Crucially, the transferring data controller must ensure that the recipient country or entity offers a level of data protection that is equivalent to or higher than that prescribed by Indonesian law. In instances where this level of protection is not guaranteed, the law requires that adequate and binding data protection measures are in place. Furthermore, if these conditions are not met, explicit consent from the data subject becomes a prerequisite for the transfer.

These articles highlight the intricate challenges and legal requirements involved in the cross-border transfer of personal data. Within the framework of decentralized data systems, such regulations present an opportunity to embed compliance mechanisms into the system architecture. Decentralized systems, with their inherent features of transparency and security, can be designed to automatically comply with these legal requirements. This includes ensuring the adequacy of data protection in cross-border transfers and obtaining necessary consents, thereby streamlining compliance processes in a global digital environment. Thus, decentralized data systems emerge as a potent tool for navigating the complex landscape of international data transfer, aligning with the rigorous standards set by Indonesia's Personal Data Protection Law.

The centralized approach to personal data management, while traditional, faces several challenges, especially when evaluated against the rigorous compliance requirements set forth in Indonesia's Personal Data Protection Law. Centralized systems, which involve a single point of control and management for data, often struggle with issues of transparency, security, and effective consent management – all key aspects underlined in the law.

For instance, Articles 21 and 22 of the law emphasize the necessity for informed and explicit consent in data processing, requiring clear communication and legal validity in obtaining consent. Centralized systems, however, may not always provide the required level of clarity and transparency, leading to potential ambiguities in consent management. Moreover, the centralized storage of consent records can be vulnerable to unauthorized access and modifications, challenging the law's demand for data integrity and secure handling.

Articles 55 and 56, addressing the transfer of personal data, both within and outside Indonesia, highlight the need for equivalent or higher data protection standards during such transfers. Centralized data systems often face difficulties in ensuring consistent protection levels across different jurisdictions, potentially leading to non-compliance with these articles. The single-point-of-failure nature of centralized systems also poses significant risks during data transfer, making it challenging to maintain continuous protection as mandated by the law.

Furthermore, the centralized approach struggles with the law's requirement for data accuracy and consistency (Article 29). In such systems, the updating and verification of data depend heavily on the central authority, which can lead to delays and errors. This centralized dependency contrasts with the law's emphasis on maintaining the integrity and reliability of personal data.

In summary, the centralized approach to personal data management often falls short in addressing the comprehensive requirements of Indonesia's Personal Data Protection Law. Issues like limited transparency, potential security vulnerabilities, challenges in managing informed consent, and difficulties in maintaining data integrity across borders, highlight the limitations of centralized systems. These problems underscore the need for more robust and compliant data management solutions, such as decentralized systems, which inherently align better with the law's stringent standards.

The decentralized approach to managing personal data presents a compelling solution to the challenges inherent in centralized systems, especially in the context of compliance with Indonesia's Personal Data Protection Law. Decentralized data management, characterized by distributed control and enhanced security features, aligns closely with the law’s rigorous standards for data protection, consent management, and data transfer.

Unlike centralized systems, decentralized architectures inherently support transparency and data integrity. In reference to Articles 21 and 22 of the law, which emphasize informed and explicit consent, decentralized systems can offer a more robust framework for obtaining and managing consent. Blockchain technology, a common feature in decentralized systems, enables transparent and immutable consent records, ensuring that the legal validity and clarity required by the law are maintained. This technology also prevents unauthorized alterations, directly addressing the law's demand for data integrity and secure handling.

Regarding the data transfer requirements stipulated in Articles 55 and 56, decentralized systems offer enhanced security during both domestic and international data transfers. The distributed nature of these systems significantly reduces the risks associated with a single point of failure, ensuring continuous protection of data in transit. Furthermore, the inherent security protocols in decentralized systems can be aligned with the varying data protection standards across jurisdictions, ensuring compliance with international data transfer regulations.

 https://doi.org/10.24912/jssh.v2i1.34245

Additionally, the decentralized approach effectively addresses the requirement for data accuracy and consistency as outlined in Article 29. In a decentralized system, data verification and updates can be managed more efficiently and transparently, with multiple nodes in the network contributing to the maintenance of data integrity. This collective approach to data management ensures a higher degree of accuracy and reliability, in line with the law's provisions.

In conclusion, decentralized data management systems offer a robust solution for aligning with the compliance requirements of Indonesia's Personal Data Protection Law. By inherently supporting transparency, security, and effective consent management, decentralized systems not only address the shortcomings of centralized approaches but also enhance the overall integrity and reliability of personal data management. This makes decentralized systems an ideal choice for organizations looking to comply with the stringent standards of data protection laws.

4. KESIMPULAN DAN SARAN

In conclusion, the enactment of Indonesia's Personal Data Protection Law marks a significant stride in the realm of data privacy and security, setting forth comprehensive and stringent standards for the management and protection of personal data. The law's detailed provisions, as exemplified in Articles 21, 22, 55, 56, and 29, emphasize informed consent, data integrity, secure data transfer, and the overall transparency of data processing activities. These requirements present a formidable challenge for traditional centralized data management systems, which often grapple with issues of data transparency, security vulnerabilities, and efficient consent management.

In contrast, decentralized data management systems emerge as a potent solution to these challenges. By leveraging the inherent advantages of distributed control and blockchain technology, decentralized systems inherently support the law's demands for transparency, data integrity, and security. These systems offer a robust framework for managing informed consent, ensuring data accuracy, and facilitating secure data transfer across jurisdictions.

Therefore, in the rapidly evolving digital landscape, where data privacy and protection are of paramount importance, decentralized data management systems not only offer a viable path to achieving compliance with Indonesia's Personal Data Protection Law but also represent a forward-thinking approach to data governance. By adopting decentralized systems, organizations can not only adhere to legal requirements but also foster greater trust and reliability in their data management practices, paving the way for a more secure and transparent digital future.

Organizations should prioritize adopting blockchain and other decentralized technologies to align with Indonesia's Personal Data Protection Law. These technologies offer transparency, security, and integrity, vital for compliance with legal requirements such as consent management and data integrity. Investment in these technologies, coupled with the development of comprehensive data governance policies, will ensure a holistic approach to data management. These policies should be tailored to integrate the law's principles, focusing on informed consent, data accuracy, and secure data transfers.

The role of training and collaboration cannot be overstated. Regular training programs for employees about data privacy laws and the operational aspects of decentralized systems are essential. Furthermore, collaboration with legal and IT experts is crucial to ensure that the technological infrastructure and policies are not only legally compliant but also technologically robust. This approach will address both the technical and legal complexities of data management.

Finally, continuous monitoring and updating of data systems are critical to adapt to evolving legal and technological landscapes. Additionally, engagement in international dialogue and cooperation is vital, especially for organizations involved in cross-border data transfers. Such engagement ensures alignment with global data protection standards, which is crucial for multinational corporations. By implementing these strategies, organizations can navigate the complexities of data protection laws effectively, ensuring compliance and fostering trust in their digital operations.

REFERENSI

Ciriani, V., De Capitani di Vimercati, S. S. F., Samarati, P., Yu, T., & Jajodia, S. (2007). *Secure data management in decentralized system*. Springer.

Hart, C. (2019). *Blockchain and data privacy*. LexMundi. https://www.lexmundi.com/media/ye2hqrsh/lex-mundi-blockchain-data-privacy.pdf.

Thomson Reuters. (2018, May 25). *Top five concerns with GDPR compliance*. Thomson Reuters. https://legal.thomsonreuters.com/en/insights/articles/top-five-concerns-gdpr-compliance &#8203.

Kennedy, G. E. (2019). Data privacy law: a practical guide to the GDPR. *(No Title)*.

Rosadi, S. D. (2023). *Pembahasan UU Pelindungan Data Pribadi (UU RI No. 27 Tahun 2022)*. Sinar Grafika.

Tapscott, D., & Tapscott, A. (2016). *Blockchain revolution: how the technology behind bitcoin is changing money, business, and the world*. Penguin.

 https://doi.org/10.24912/jssh.v2i1.34245