Research article
UDC 34:004:346.6:004.7
EDN: https://elibrary.ru/lqycmn
DOI: https://doi.org/10.21202/jdtl.2025.12

Pseudonymization of Personal Data of Crypto Assets Users: Issues of Legal Regulation in Indonesia

I Komang Oki Mayuna ✉
Brawijaya University, Malang, Indonesia

Reka Dewantara
Brawijaya University, Malang, Indonesia

Patricia Audrey Ruslijanto
Brawijaya University, Malang, Indonesia

Keywords

blockchain technology,
crypto assets,
cryptocurrency,
digital technologies,
law,
legislation,
personal data protection,
personal data,
pseudonymization,
trading in crypto assets

Abstract

Objective: to analyze the possibility of providing legal protection for pseudonymized personal data of crypto assets users in the legal system of Indonesia.

Methods: the work uses a comprehensive legal analysis based on the study of the current regulatory legal acts of Indonesia in the field of personal data protection. The research was carried out using legislative, conceptual and comparative methodological approaches, including an analysis of the Indonesian Law on Personal Data Protection, the EU General Regulation on Personal Data Protection, and the British Data Protection Act.

Results: it was established that pseudonymization of crypto assets user data in Indonesia is feasible from a legal point of view; however, the existing legislation contains significant gaps. The current Indonesian Personal Data Protection Law does not recognize pseudonymized data as a separate category of personal data subject to legal protection. The authors point out the problems with the implementation of the rule for controlling transfers of crypto assets by physical traders. As additional information for the re-identification of pseudonymized data is not stored separately, it increases the risks of privacy violations.

✉ Corresponding author

Scientific novelty: the authors provide a comprehensive analysis of the legal mechanisms for protecting pseudonymized data in the context of cryptocurrency transactions. A conceptual model is proposed for improving national legislation on personal data protection. It implies including pseudonymized data as a separate category of protected information. Recommendations are given, which establish criteria for the legitimate re-identification of pseudonymized data to ensure legal certainty in the field of protecting crypto assets users.

Practical significance: the research results can serve as a theoretical and methodological basis for reforming the Indonesian Law on Personal Data Protection and creating an effective legal mechanism for protecting crypto assets users. The proposed amendments to Article 4 of the said Law will make it possible to include pseudonymized data in the list of protected categories of personal data, which will provide legal certainty for participants in the cryptocurrency market and increase the level of their personal data protection in the digital economy.

For citation

Mayuna, I K. O., Dewantara, R., & Ruslijanto, P. A. (2025). Pseudonymization of Personal Data of Crypto Assets Users: Issues of Legal Regulation in Indonesia. *Journal of Digital Technologies and Law, 3*(2), 275–303. https://doi.org/10.21202/jdtl.2025.12

Contents

Introduction

The payment system has evolved; initially, it relied on physical money but now shifts to e-money. The world was recently shocked by the emergence of cryptocurrency, which is used as a payment method in trade transactions (Jati & Zulfikar, 2021). However, not all countries, including Indonesia, recognize cryptocurrency as a legal means of payment. Cryptocurrency in Indonesia cannot be used as a legal means of payment because, based on Article 2 of Law Number 7 of 2011 concerning Currency, it is stated that the official currency of Indonesia is the rupiah (Setiawan et al., 2023). However, cryptocurrency in Indonesia has been recognized as an investment instrument, as explained in Article 1 of the Minister of Trade Regulation Number 99 of 2018 concerning the General Policy for Implementing Crypto Asset Futures Trading (Crypto Asset). Therefore, in Indonesia, cryptocurrency is called a "crypto asset" (Ulya & Pambudi, 2024).

Crypto asset transactions are closely related to pseudonymisation data processing. When crypto asset investors transfer crypto assets to a digital wallet, either in the form of assets or conversion to fiat money (IDR), the transaction is recorded in the blockchain system using a pseudonymisation wallet address or public address. On the other hand, these transactions are also recorded or stored by physical traders of crypto assets as part of the implementation of the travel rule principle, as regulated in Article 38, paragraph (1) of BAPPEBTI Regulation Number 13 of 2022 concerning Amendments to BAPPEBTI Regulation Number 8 of 2021.

As a result, pseudonymisation data processing is carried out by physical crypto asset traders. However, additional information that could be used for re-identification is not stored separately from the pseudonymisation data, increasing the risk of data leakage. A pseudonym can still be linked to the data subject's identity. Moreover, research has shown that data stored within blockchains can be traced back to natural persons (obfuscated personal data subjects) if processed using adequate technical methods, potentially revealing the identity of the subject who owns the pseudonymisation data.

Unfortunately, the Personal Data Protection Law does not recognize pseudonymisation data as a type that qualifies for protection. Therefore, it is necessary to regulate pseudonymisation data as one of the categories protected under the Personal Data Protection Law to ensure legal safeguards for crypto asset investors.

1. Concept of personal data protection

1.1. Personal data protection

Personal data protection cannot be separated from the definition of data. In Latin, data is called datum, a part of information. The collection of data leads to the formation of information. In the context of personal data, different countries use different terms; some refer to it as "personal information", while others use it as "personal data". However, substantively, both terms have nearly the same meaning. Aside from these terminological

differences, there are also variations in the interpretation of the concept of personal data itself[1]. Indonesia uses the term "personal data", based on Article 1, Number 1 of the PDP Law[2]: "Personal data refers to information about an individual who is identified or can be identified, either individually or in combination with other information, directly or indirectly, through electronic or non-electronic systems".

The provisions in the PDP Law define personal data as information that can be identified or is identifiable through electronic or non-electronic means. In contrast, the GDPR does not specify this distinction.

Personal data protection encompasses at least two key concepts: securing physical personal data and establishing regulations that provide privacy guarantees for using a data subject's data. Fundamentally, data protection is closely related to safeguarding the right to privacy (Yetno, 2021). This is also emphasized by Alan Westin, who stated that data privacy is the right of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them will be communicated or collected by others[3].

Conceptually, establishing an absolute or standard definition of privacy is challenging, as the term remains a subject of ongoing debate among experts. Privacy refers to an individual's right to control personal information collection, use, disclosure, and retention (Jose, 2023). The concept of privacy was first introduced by Samuel Warren and Louis Brandeis, who stated that a fundamental human right must be protected, known as "The Right to Privacy", which means the following (Anand et al., 2020): "Privacy is the right to enjoy life and the right to be left alone and this development of the law was inevitable and demanded of legal recognition".

Based on this explanation, the right to privacy encompasses the right to enjoy life, to be left alone, and to seek legal protection for one's privacy. According to the Big Indonesian Dictionary, privacy is defined as freedom or personal freedom. Warren and Brandeis further emphasize that privacy is the right to enjoy life and be left alone, ensuring everyone has the right to maintain their privacy (Dewi, 2017). Therefore, the right to privacy is the fundamental human right of every individual to maintain confidentiality and security (Anggen Suari & Sarjana, 2023). Everyone's privacy must be protected because an individual's privacy is compromised when personal information is made public. Therefore, privacy protection

1 Djafar, W., Sumigar, B. R. F., & Setianti, B. L. (2016). Perlindungan Data Pribadi Usulan Pelembagaan Kebijakan Dari Perspektif Hak Asasi Manusia. Lembaga Studi dan Advokasi Masyarakat.

2 Undang – Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi. Pasal 1 angka 1. (2022). Lembaran Negara Republik Indonesia, 196, Tambahan Lembaran Negara Republik Indonesia, 6820.

3 https://clck.ru/3MEF5G

is essential. However, many experts find it challenging to define and limit the concept of privacy due to its broad scope. As a result, many countries combine the idea of privacy with protecting personal data. This aligns with modern privacy theory, which Alan Westin first developed in his book Privacy and Freedom, where he states that (Pelteret & Ophoff, 2016): "Privacy is the claim of individuals, group or istitution to determine for themselves when, how, and to what extent information about them is communicated to others".

Based on this statement, privacy is the right of individuals, groups, or institutions to determine whether or not data about them will be communicated to other parties. Legal experts further developed this definition in response to information and communication technology advances, where an individual's privacy data can be accessed, processed, collected, and manipulated. As a result, one type of privacy right became known as personal data privacy.

The 1945 Constitution of the Republic of Indonesia (UUD NRI 1945) regulates the protection of human rights. After the amendment to the 1945 Constitution, the regulation of citizens' human rights became more comprehensive compared to the pre-amendment Constitution, which only addressed them in general and brief terms. The amendments to the 1945 NRI Constitution now include guarantees for protecting and fulfilling citizens' rights, one of which is the right to privacy (Asrun, 2016). The protection of the right to privacy is not explicitly regulated in the 1945 NRI Constitution. Still, the right to privacy is implicitly protected under Article 28G, paragraph (1) of the 1945 NRI Constitution, which states that[4]: "Every person has the right to protect themselves, their family, honor, dignity, and property under their control, and has the right to a sense of security and protection from the threat or fear of doing or not doing something, which is a human right".

Based on the explanation above, the right to privacy is implicitly regulated in this article. The explanation of this article aligns with the concepts of privacy discussed earlier, which include the right to honor, dignity, and property, as well as the right to a sense of security and protection from threats. In addition, privacy guarantees are also regulated in Article 29, paragraph (1), and Article 30 of Law Number 39 of 1999 concerning Human Rights. However, Indonesian laws and regulations do not define the right to privacy (Rohmansyah et al., 2023).

The right to privacy is related to personal data, where personal data is one of the elements protected by law. Thus, everyone has the right to maintain their personal data's privacy (confidentiality and security) (Priskarini et al., 2019). The European Human Rights Court also stated that the protection of personal data is fundamental and that respect for a person's right to privacy is as regulated in Article 8 of the European Convention on Human Rights (European Convention on Human Rights and Fundamental Freedoms) (Sinaga & Putri, 2020). This is also in line with the provisions of Article 28G, paragraph (1)

[4] Undang – Undang Dasar Negara Republik Indonesia Tahun. (1945). Pasal 28G ayat (1).

of the 1945 Constitution of the Republic of Indonesia, which protects personal data as part of the right to privacy. Although Article 28G, paragraph (1) of the 1945 Constitution of the Republic of Indonesia does not explicitly mention the right to privacy, this provision implies a guarantee of the right to privacy (Soraja, 2021).

Apart from that, the explanation of Article 26 of the ITE Law Number 19 of 2016 clarifies that protecting personal data is one aspect of personal rights (privacy rights) (Priliasari, 2023). So, personal data protection is part of each individual's right to privacy. The PDP Law defines personal data protection, as explained in Article 1, number 2 of the PDP Law, which states that:[5] "Personal Data Protection is the overall effort to protect Personal Data during Personal Data processing to guarantee the constitutional rights of Personal Data subjects".

Based on this explanation, the right to protect personal data is a constitutional right of Indonesian citizens that the state must safeguard. Therefore, personal data protection is part of the right to privacy, implicitly protected under Article 28G paragraph (1) of the 1945 Constitution of the Republic of Indonesia. Consequently, personal data protection is a constitutional right of citizens that the state must uphold to ensure they receive their rights. Thus, personal data is an inseparable part of the right to privacy, as protecting personal data is an integral aspect of the right to privacy guaranteed by the 1945 Constitution of the Republic of Indonesia.

1.2. Meaning of pseudonymisation data

The definition of a pseudonym in the Big Indonesian Dictionary refers to a name used to conceal one's true identity (pseudonym). Pseudonymisation of data involves replacing identifying characteristics with pseudonyms or, in other words, modifying the data so that the data subject cannot be directly identified. This pseudonymisation can only be associated with confidential identification data (additional data).

Pseudonymisation emphasizes techniques that replace, delete, or alter information that identifies an individual while keeping that information separate. Data that has undergone the pseudonymisation process remains classified as personal data and falls within the scope of data protection law.

Pseudonymisation begins with original data, which is then disguised, resulting in two data sets: pseudonymized data and additional information. Both datasets can be used to reconstruct the original data. This means that pseudonymized data can be linked back to the original data of the data subject using additional information. Thus, pseudonymisation data retains data protection principles.

[5] Undang – Undang Nomor 27, Pasal 1 angka 2. (2022), tentang Perlindungan Data Pribadi, Lembaran Negara Republik Indonesia Tahun, 196, Tambahan Lembaran Negara Republik Indonesia, 6820.

Article 4, paragraph (5) of the GDPR defines pseudonymisation as follows: "pseudonymisation means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person"[6].

As explained above, pseudonymized personal data falls within the scope of the GDPR. This definition clearly describes and emphasizes that data undergoing the pseudonymisation process begins and remains classified as personal data. Pseudonymisation data is still associated with a natural person who can be identified according to the definition of personal data itself. The pseudonymisation process only prevents the direct identification of the pseudonymisation data subject (Mourby et al., 2018).

Pseudonymisation, as described in Article 4, paragraph (5) of the GDPR, refers to processing personal data so that it can no longer be associated with a specific data subject without using additional information. Such additional information must be kept separately and subject to technical and organizational measures to ensure that personal data is not linked to an identifiable person. This provision clearly distinguishes between anonymized data and pseudonymisation data. In the case of anonymous data, data protection principles do not apply because the subject is not or can no longer be identified. In contrast, pseudonymisation data must adhere to data protection principles because the data belongs to an identifiable individual (Bolognini & Bistolfi, 2017). This is also explained in Recital 26 of the General Data Protection Regulation (GDPR), which states: "The principles of data protection should apply to any information concerning an identified or identifiable natural person; personal data which has undergone pseudonymisation, which could be attributed to a natural person by the use of additional information, should be considered to be information on an identifiable natural person..." (Finck & Pallas, 2020).

So, even though pseudonymisation data can be reconnected to the original data of the data owner, processors and personal data controllers must ensure that any additional information used for re-identification is stored separately. This ensures that other parties cannot access or use it without permission to re-identify the original data of the subject that has undergone the pseudonymisation process (Huang & Zheng, 2023). Therefore, re-identification can be prevented by ensuring that unauthorized parties do not gain access to additional data or information that could be used to identify the pseudonymized data (Kohlmayer et al., 2019).

[6] General Data Protection Regulation (EU GDPR). (2018, May 23). GDPR-Text.com. https://goo.su/Ke5Byw

Pseudonymisation is used as a new approach to controlling data distribution to maintain the data owner's privacy by applying pseudonyms, which hide the relationship between the information and the data owner. This pseudonymisation aims to control the flow of information to individuals to prevent the misuse of their information or privacy. Additionally, pseudonymisation also functions to limit unwanted data disclosure by unauthorized parties. One method of implementing pseudonymisation is encryption. Data that undergoes the encryption process is transformed into specific codes that generate a public key (Suryawijaya, 2023). Pseudonymisation can address privacy issues (personal data protection), confidentiality, and integrity. The scope of a pseudonym includes knowledge or information related to the holder and the pseudonym. Information about pseudonyms must only be known by the holder or an authorized party because it can refer to the data subject and reveal their identity if identified with additional data (Kumar Rai, 2016).

1.3. Meaning of anonymized data

Anonymization is replacing, modifying, or deleting individual data or information so that it cannot be re-identified. Therefore, pseudonymisation differs from anonymization in that information processed through pseudonymisation is not entirely deleted or disguised but is only replaced with a pseudonym, allowing it to be re-identified with the help of additional information stored separately. Meanwhile, anonymization not only removes names but typically disguises or completely deletes a person's information, making it impossible to identify the data subject (Hintze & El Emam, 2018).

Pseudonymisation and anonymization are two distinct terms, but they are often confused in the context of personal data protection. Data that undergoes an anonymization process will remove any information that could serve as an identifier for the data subject. In other words, anonymous data permanently disconnects the personal data from a specific identified or identifiable person. Meanwhile, pseudonymization does not remove all identifying information from the data but only reduces the association of the data set with a person's real identity (Štarchoň & Pikulík, 2019). The EU Article 29 Working Party also explains that "Pseudonymisation is not an anonymization method, as pseudonymisation only reduces the linkage of a data set with the original data of the data subject's identity"»[7]. Thus, data will be considered anonymous if the data that undergoes de-identification cannot be changed or re-identified to the subject who owns the data (Mourby et al., 2018).

[7] EU. (1995, October 24). Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. https://clck.ru/3MEFan

Anonymization is intended to prevent the re-identification of data or individuals who have gone through the anonymization process. Thus, anonymous data does not fall under data protection principles. This is also explained in Recital 26 of the GDPR, which states that...: "…The principles of data protection should therefore not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable…"[8].

Therefore, anonymous data does not fall under the principles of personal data protection because it cannot be linked back to a specific identified or identifiable person. On the other hand, pseudonymisation data still falls under the principles of personal data protection because it can be linked back to an identified or identifiable natural person. Thus, the GDPR obligates personal data controllers to separate additional information that can be used to re-identify pseudonymisation data. In addition, the controller is also obliged to consider all possible means or methods that specific individuals could use to re-identify pseudonymisation data.

1.4. Meaning of aggregated data

Aggregate data is data produced through an aggregation process (grouping data). Data aggregation is collecting and presenting raw data in summary form for statistical analysis. Aggregate data is generally known as statistical data and is usually displayed as tables, charts, graphs, or bar charts (Sinulingga, 2022). Therefore, aggregate data does not fall under personal data protection because aggregate data cannot re-identify a person's identity. This is also explained in Recital 26 of the GDPR, which states that: "…This Regulation does not therefore concern the processing of such anonymous information, including for statistical or research purposes"[9].

Thus, based on the explanation above, of the three types of data, namely pseudodonymisation data, anonymous data, and aggregate data, only pseudodonymisation data is subject to the principles of personal data protection. This is because pseudonymisation data can be identified as the original data of the owner, with additional information stored separately.

8 Resital 26 General Data Protection Regulation. (2022).

9 Ibid.

2. The relationship between pseudonymized data protection of crypto asset customers and crypto asset trading

Cryptocurrency is a currency not centralized by banks; it is created using computer encryption technology recorded on a blockchain platform. Users use cryptocurrency to store and make transactions, although not all countries legalize cryptocurrency as a means of payment in trade transactions. For example, as regulated in Article 2 of Law Number 7 of 2011, Indonesia stipulates that the legal means of payment is the rupiah (Setiawan et al., 2023). So, in this case, cryptocurrency is not a legal currency in Indonesia that can be used as a means of payment. This was also expressly stated by Bank Indonesia, which declared that cryptocurrency cannot be used as a means of payment in Indonesia. Furthermore, the prohibition on crypto assets as a means of payment in Indonesia is explicitly regulated in Bank Indonesia Regulation Number 20 of 2018 concerning Electronic Money (Chang, 2019).

On the other hand, cryptocurrency can be used as an investment instrument in Indonesia, as explained in Article 1 of the Minister of Trade Regulation Number 99 of 2018 concerning the General Policy for Implementing Crypto Asset Futures Trading (Crypto Asset). Thus, cryptocurrency is recognized as a "Crypto Asset" in Indonesia (Ulya & Pambudi, 2024). Crypto assets can be defined as private assets that rely on a blockchain system to secure digital value or contractual rights. These assets can be transferred, stored, or traded electronically. Abroad, crypto assets are usually known as cryptocurrency, and cryptocurrency can be used as virtual currency in buying and selling transactions (Pudjastuti & Westra, 2021). Meanwhile, crypto assets can only be used as investment instruments in Indonesia.

Crypto assets are digital currency systems that are secured using cryptographic techniques (Faozi & Segara Gustanto, 2022). Cryptography refers to encryption, which converts text into signs or symbols. Cryptocurrency uses a technology called blockchain (Ausop & Aulia, 2018). Therefore, cryptocurrency is a digital currency that stores digital data related to users' crypto asset transactions in the blockchain system. Thus, cryptocurrency cannot be separated from the blockchain because it is connected, with the blockchain functioning as a data storage system for crypto asset investors.

In computer systems, there are three types of networks, one of which is a distributed network. Distributed systems are not subject to any central authority, so each system node is part of a network and is directly connected to other system nodes (Suryawijaya, 2023).

Blockchain implements a distributed system, so all system nodes in the network have the same rights and obligations to store information and are connected (Handoko et al., 2024). Blockchain-based systems offer a higher level of transparency compared to existing records and ledgers. Because of this transparency, changes are visible to everyone on the network, and transactions cannot be changed or deleted once they are entered into the blockchain. Blockchain provides transparency to everyone in the network, allowing them to see the transactions in the blockchain system (Nanda Sari & Gelar, 2024).

Besides that, blockchain also implements a decentralized system, which aims to eliminate the involvement of intermediaries (third parties), thereby increasing transparency and trust in the system (Abdul Karim & Hadinata, 2023). Decentralized blockchain essentially allows everyone to connect to the network so that they have access to the blockchain system (Suryawijaya, 2023). What's more, data that has been entered into the blockchain cannot be changed or deleted. Data in blocks entered into the blockchain system can also be traced back to previous blocks. With this blockchain system, transactions carried out in the past cannot be changed, so they still leave clear traces. However, security in blockchain systems is not perfect. This is because the blockchain system is transparent and decentralized, meaning everyone can see transactions in the blockchain network (Jamwal et al., 2024). Therefore, many experts study blockchain because it is considered that security in blockchain technology is not yet entirely perfect for protecting blockchain users' data, as stated by researchers from the Open Data Institute (Utomo, 2022).

However, many users feel that this transparency is not a problem for privacy because of pseudonymization, where only users with the private key can use it to redescribe the public key. However, in the concept of personal data protection, the controller must be able to guarantee that the data stored is kept confidential and available and that only authorized parties can access the data. In reality, however, the data entered into the blockchain system contradicts the principles of confidentiality and availability because everyone can see the data entered into the blockchain system, as the blockchain is transparent (Tatar et al., 2020). Even though the data entered into the blockchain system is Pseudonymisation, research has shown that the data found in the blockchain can refer to individual people (disguised personal data subjects) if this is done by connecting data available on the blockchain network to data outside the network or by analyzing the context of transactions that occur on the blockchain using network analysis. Moreover, the user's real identity can also be revealed when using information outside the network. Furthermore, if additional data is not stored separately from the public key, it can reveal the user's real identity. For example, a study shows that it is still possible to re-identify crypto asset customers by tracking pseudonymous wallet addresses and transactional data in the blockchain system (Tatar et al., 2020).

Therefore, crypto assets are closely related to the processing of pseudonymisation data. In the crypto asset trading transaction mechanism, crypto asset transactions are closely related to the pseudonymisation data process. When crypto asset investors carry out transactions (exchange or transfer) of crypto assets, whether from crypto assets to fiat money (IDR) or vice versa, or from one crypto asset to another, the transaction will be entered into the blockchain system in the form of a pseudonymisation public address/wallet address. As a result, everyone in the blockchain system can see transactions made by crypto asset investors, even though they won't know the identity of the user who created the transaction, as the public address/wallet address entered into the blockchain system is Pseudonymisation. Furthermore, the transaction will also be recorded or saved by the crypto asset trader as a financial record, which will be reported to CoFTRA to prevent crypto asset transactions from being used as a mode for committing criminal acts such as money laundering.

Thus, the physical trading of crypto assets cannot be separated from processing personal data in pseudonymisation data, especially regarding pseudonymisation data protection. This is because crypto asset trading transactions involve pseudonymous wallet addresses recorded in the blockchain system. Moreover, physical crypto asset traders are required to apply the Know Your Customer (KYC) principle, which involves collecting customer personal data as part of anti-money laundering programs and efforts to prevent the financing of terrorism and the proliferation of weapons of mass destruction. Therefore, personal data collection activities by crypto asset traders can result in "additional information" that may be used to re-identify the pseudonymisation data of crypto asset customers (Atikah, 2023).

In addition, pseudonymous wallet addresses are collected by physical crypto asset traders as a form of applying the travel rule principle. The travel rule is a regulation that requires virtual asset service providers (crypto asset traders) to collect, store, and transmit certain information about the sending and receiving assets in every transaction carried out, including transactions that cross jurisdictional boundaries (Maulana, 2024). This is in line with on-chain crypto asset trading transactions, where the user's public address/wallet address is recorded in the blockchain system and on the platform used by crypto asset customers to carry out crypto asset trading transactions. This raises the risk that the crypto asset customer's public address/wallet address may be re-identified with additional information obtained and collected by the crypto asset trader as part of implementing the know your customer (KYC) principle (Alfin et al., 2024).

Thus, personal data is processed in pseudonymous form and carried out by physical crypto asset traders. However, the implementation of the travel rule principle does not consider the principle of protecting personal data in pseudonymisation form, where "additional information" that can be used for re-identification should be stored separately. Therefore, crypto asset trading is closely related to protecting the pseudonymisation data of crypto asset investors. Hence, regulations must guarantee the protection of crypto asset investors' pseudonymisation data processing in the crypto asset transaction process.

3. Data pseudonymization and reidentification regulations

3.1. Indonesian Personal Data Protection Law

The protection of personal data is a constitutional right of Indonesian citizens. This is also confirmed in Article 1, number 2 of the PDP Law, which states that personal data protection is the overall effort to protect personal data in processing personal data to guarantee the constitutional rights of personal data subjects. The personal data in question refers to data about natural persons who are identified or can be identified individually or in combination with other information, either directly or indirectly, through electronic or non-electronic systems. Based on the explanation of Article 1, point 1 of the PDP Law, this article indirectly accommodates the meaning of pseudonymisation

data. Pseudonymisation data refers to the alteration or replacement of identifying data characteristics with a pseudonym so that it does not allow the data subject to be identified directly without the help of additional information stored separately.

Unfortunately, the PDP Law does not regulate pseudonymisation data as one of the types of data that receives protection. This can be seen from the provisions of Article 4, paragraph (1) of the PDP Law, which divides personal data into two types: specific and general personal data. Specific personal data includes health data and information, biometric data, genetic data, criminal records, children's data, personal financial data, and other data by statutory provisions. Meanwhile, general personal data includes full name, gender, nationality, religion, marital status, and/or personal data combined to identify a person (Adhiwisaksana & Allagan, 2023). However, both types of personal data, specific and general personal data, do not include pseudonymisation data as part of the personal data that receive protection.

Even though Article 4, paragraph (3), letter f of the PDP Law includes "personal data combined to identify a person", the Elucidation to Article 4, paragraph (3), letter f of the PDP Law only includes cell phone numbers and IP addresses. Implicitly, "personal data combined to identify a person" means that the data functions to identify or link the individual owner of the personal data. Therefore, it fundamentally differs from pseudonymisation data, which is not intended to identify or link natural persons. Instead, pseudonymisation data is meant to disguise the data subject's identity, making re-identification impossible without using additional information that is stored separately.

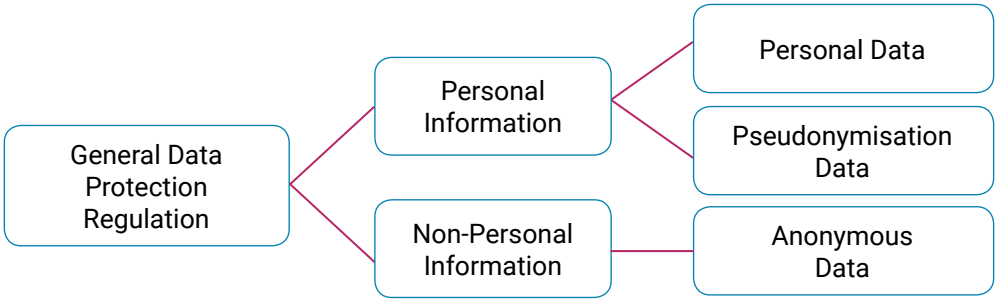
Moreover, the PDP Law also does not regulate the re-identification criteria considered valid for pseudonymisation data. Additionally, the PDP Law does not regulate the requirements for processing pseudonymisation data that has been re-identified and is considered valid. The PDP Law does not address pseudonymisation data as data subject to data protection principles. Thus, the PDP Law does not regulate the re-identification and processing of re-identified personal data, which could result in personal data violations.

3.2. General Data Protection Regulation

The European Union issued the General Data Protection Regulation (GDPR), which includes regulations related to de-identification, one of which is pseudonymisation. The GDPR introduced the concept of pseudonymisation and contributed to popularizing the idea of pseudonymisation data, which falls between personal data and anonymous data. The GDPR emphasizes that the storage and protection of additional information must be carried out separately in the definition of pseudonymisation information. This is explained in Article 4, paragraph (5) of the GDPR (Joo & Kwon, 2023).

Article 4, paragraph (1) GDPR defines personal data, as "any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier

such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person" (Imakura et al., 2023). The personal data subject to data protection principles according to GDPR are as follows (Joo & Kwon, 2023):



The personal data subject to data protection principles

Sourse: (Joo & Kwon, 2023).

The GDPR protects pseudonymisation data, which is not considered anonymous because it can be identified or re-identified using additional information that must be stored separately (Limniotis, 2021). The GDPR provides data protection principles for pseudonymisation data, as explained in Recital 26 of the GDPR, which states: "The principles of data protection should apply to any information concerning an identified or identifiable natural person; personal data which has undergone pseudonymisation, which could be attributed to a natural person by the use of additional information, should be considered to be information on an identifiable natural person"[10]. The European Union includes pseudonymisation data within the scope of "personal data", so pseudonymisation data is protected by law (Wahyuningtyas, 2024).

However, the GDPR does not provide data protection principles for anonymous data, as explained in Recital 26 of the GDPR, which states: "...The principles of data protection should therefore not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable..."[11]. This is because, in essence, anonymous data is intended to prevent re-identification, so data that has gone through the anonymization process cannot be linked or re-identified to a particular individual (Dat & An, 2024).

Therefore, Article 29 of GDPR obligates data controllers to separate additional information that can be used to link personal data that has undergone a pseudonymisation process. Additionally, the controller must also consider all means or methods that may be used by certain parties to re-identify pseudonymisation data. This is a form

[10] Resital 26 General Data Protection Regulation. (2022).

[11] Ibid.

of legal protection against pseudonymisation data processing (Finck & Pallas, 2020). Unfortunately, the GDPR does not provide further regulations regarding the criteria for re-identification of pseudonymisation data that is considered valid. On the other hand, the GDPR obligates member countries to establish legal rules that apply to violations of the provisions of the GDPR, as regulated in Article 84 paragraph (1) of the GDPR.

3.3. Data Protection Act 2018

The General Data Protection Regulation (GDPR) affects European Union countries, requiring them to adopt the GDPR into their respective national personal data protection laws. Therefore, the GDPR obligates member countries to establish legal rules that apply to violations of its provisions, as regulated in Article 84 paragraph (1) of the GDPR. In addition, member countries must also encourage the preparation of codes of ethics that can support the implementation of the GDPR, one of which is related to pseudonymisation data, as regulated in Article 40 paragraph (2) letter d of the GDPR. Consequently, the UK established data protection regulations, namely the Data Protection Act 2018, which regulates the re-identification of pseudonymisation data. Article 171, paragraph (2) of the UK DPA 2018 defines de-identification and re-identification as follows[12]:

"(a) personal data is "de-identified" if it has been processed in such a manner that it can no longer be attributed, without more, to a specific data subject;

(b) a person "re-identifies" information if the person takes steps which result in the information no longer being de-identified within the meaning of paragraph (a)".

Any person who re-identifies information that constitutes personal data, which has been de-identified (pseudonymized) without the consent of the controller or responsible controller or supervisor, constitutes a personal data violation, as regulated in Article 171 paragraph (1) of the DPA 2018. Therefore, provisions in paragraphs (1) and (2) of Article 171 of the DPA 2018 refer to or represent pseudonymization as outlined in Article 4, paragraph (5) of the GDPR. Thus, anyone who re-identifies pseudonymisation data is considered to have committed a personal data violation.

However, the 2018 DPA provides criteria for re-identification that are considered valid, one of which is for the public interest, including the purpose of preventing or detecting crime, when required or permitted by law or court order, and in the public interest, as regulated in Article 171 paragraph (3) of the 2018 DPA. In addition, identification is considered valid if it is based on reasonable confidence and for special purposes such as academic research, as regulated in Article 171 paragraph (4). Furthermore, the 2018 DPA also regulates personal data violations concerning the processing of re-identified personal data if it turns out that the data processing was carried out without permission from the responsible party and the re-identification violates the provisions of Article 171 paragraph (1) of the 2018 DPA.

[12] Data Protection Act. (2018), Article 171 Paragraph (2).

The 2018 DPA also provides criteria for processing re-identified personal data that is considered lawful, namely for the public interest, which includes the purpose of preventing or detecting crime, required or permitted by law or court order, and in the public interest, as regulated in Article 171 paragraph (6) of the 2018 DPA. In addition, processing re-identified personal data is considered lawful if it is based on reasonable belief and for specific purposes, such as academic research, as regulated in Article 171 paragraph (7). However, Article 171 paragraph (7) does not include “effectiveness testing” as one of the criteria, whereas in Article 171 paragraph (4), “effectiveness testing” is included in the criteria for re-identification that is considered valid.

4. Crypto asset customers' pseudonymisation data protection challenges in Indonesia

The right to privacy is every person’s right to live without interference in their private life, whether by other people or the state. Thus, the state is responsible and obligated to regulate and recognize these rights. Privacy, as a right inherent to humans, can be divided into several types, one of which is information privacy. Information considered private can come in various forms depending on its intended use. Simson Garfinkel divides it into five types: personal information, private information, personal identity information, pseudonymous or anonymous information, and aggregate information (Syailendra et al., 2024).

The right to privacy is implicitly regulated in Article 28G paragraph (1) of the 1945 Constitution of the Republic of Indonesia. Protecting personal data is closely related to the right to privacy, as it constitutes one type of privacy right. Therefore, personal data protection is part of human rights, as regulated in Article 28G paragraph (1) of the 1945 Constitution of the Republic of Indonesia (Priskarini et al., 2019). Therefore, Indonesia established the Personal Data Protection Law as a form of protection for human rights, specifically the right to privacy.

Unfortunately, the PDP Law cannot fully provide legal protection regarding pseudonymisation data processing, particularly for crypto asset customers. This is because the PDP Law does not regulate pseudonymisation data as one of the types of data that receives protection. Thus, the PDP Law, particularly Article 4, which governs types of personal data, does not yet accommodate the regulation of “pseudonymisation data” as a protected data type. Even though Article 4 paragraph (3) letter f states “personal data combined to identify a person”, the Elucidation to Article 4 paragraph (3) letter f only includes cell phone numbers and IP addresses. Furthermore, pseudonymisation data is not intended to identify a person but to disguise the subject’s identity, making direct identification impossible without using additional information stored separately.

Thus, the PDP Law cannot fully guarantee personal data protection for crypto asset customers by processing personal data as pseudonymisation data. Crypto

asset transactions are closely related to the processing of personal data in the form of pseudonymisation data because transactions (exchange or transfer) of crypto assets, whether from crypto assets to fiat money (IDR) or vice versa, and from one crypto asset to another, will be recorded in the blockchain system as a pseudonymisation public address or wallet address.

Furthermore, the transaction will also be recorded or stored by the crypto asset trader in the form of sender and user names, sender and recipient wallet addresses, and sender and user addresses as a form of application of the travel rule principle. This aligns with on-chain crypto asset trading transactions, where the user's public address/ wallet address is recorded in the blockchain system and, of course, on the platform crypto asset customers use for trading transactions.

Therefore, this processing poses a risk because the crypto asset customer's public address/wallet address could be re-identified using additional information obtained and collected by the crypto asset trader as part of implementing the know your customer (KYC) principle (Alfin et al., 2024). Thus, there are personal data collection activities in the form of pseudonymisation data, which are carried out together with "additional information" that can be used to re-identify the pseudonymisation data of crypto asset customers (Atikah, 2023).

Personal data protection in electronic systems must be carried out by respecting the privacy rights of personal data owners, as personal data is private. Thus, electronic system organizers, in this case, physical traders of crypto assets, must protect the electronic information collected as a form of application of the travel rule or know-your-customer principles (Utomo, 2020). Unfortunately, the PDP Law cannot guarantee protection for processing personal data in the form of pseudonymisation data because, in essence, the PDP Law does not regulate pseudonymisation data as one type of data with protection principles. Thus, this presents a challenge for protecting pseudonymisation data for crypto asset customers because the PDP Law does not yet accommodate legal protection arrangements for processing personal data in pseudonymisation data.

Therefore, it is necessary to reformulate the PDP Law regarding regulating the types of data that receive protection to ensure legal protection for crypto asset customers. This aligns with the theory of legal protection put forward by Philipus M. Hadjon, namely the theory of preventive legal protection, which involves establishing regulations that can protect every citizen (Tirtakoesoemah & Arafat, 2019). Therefore, it is necessary to establish regulations that govern pseudonymisation data as one type that receives protection in the PDP Law as a guarantee of legal protection provided by the government to crypto asset customers against processing personal data in the form of pseudonymisation data.

This arrangement can provide legal certainty regarding legal protection for crypto asset customers by processing personal data as pseudonymisation data by physical

traders of crypto assets. In reality, crypto asset customers currently do not obtain legal protection against processing personal data through pseudonymisation data by applying the travel rule principle. Additionally, storing "additional information", which can be used to identify pseudonymisation data, is not carried out separately, making it vulnerable to exploitation by parties not authorized to re-identify pseudonymisation data illegally (Ayunda, 2022).

Moreover, the number of crypto asset customers reported by the Republic of Indonesia Ministry of Trade website reached 21.27 million people from February 2021 to September 2024. Although Pseudonymisation data leaks are currently not known to have occurred in Indonesia, crypto-news websites have suspected or claimed that the personal information of 13 million Binance users, including names, emails, telephone numbers, and residential addresses, has been leaked. However, personal data leaks in the form of names, emails, and telephone numbers can be a significant trigger for pseudonymisation data leaks. This data can be used as "additional information" to re-identify the individuals who own the pseudonymisation data.

In addition, re-identifying pseudonymisation data can also result in hacking crypto asset customers' private addresses (private key compromise). A private key compromise refers to unauthorized access by a particular person to a crypto asset customer's private key. After investigation, it was discovered that 19 cases of private key compromise had occurred, resulting in financial losses of $641.54 million in 2022 and $231.00 million in 2023 (Multazam et al., 2024). Therefore, Indonesia needs to build a robust and coordinated information technology legal system to achieve legal certainty regarding protecting crypto asset customers by processing personal data in pseudonymisation form.

This aligns with the legal convergence theory put forward by Danrivanto Budhijanto, who adapted the 4C Convergence theory. The legal convergence theory focuses on the unification of technological, economic, and legal variables in human relations in the digital era. It highlights the need for the formation of laws, both at the national and international levels, to accommodate these technological developments (Rizko Ramadoni et al., 2021). Research has shown that data found in blockchains can refer to natural persons (obfuscated personal data subjects) if handled in an adequate technical manner. This can be done by connecting data available on the blockchain network to data outside the network and analyzing the context of transactions that occur on the blockchain through network analysis. Furthermore, the user's real identity can be revealed when using information outside the network (Jamwal et al., 2024).

Thus, it is necessary to regulate pseudonymisation data in the PDP Law to guarantee legal certainty regarding the legal protection of crypto asset customers' pseudonymisation data processing. Since the PDP Law does not regulate it, it poses a challenge or obstacle for crypto asset customers to obtain legal protection concerning pseudonymisation data processing.

Conclusions

Protection of personal data is part of the right to privacy, which is implicitly regulated in Article 28G paragraph (1) of the 1945 Constitution of the Republic of Indonesia as part of the human rights of Indonesian citizens. Therefore, the state must protect the processing of its citizens' data, including that of crypto asset customers. Physical crypto asset trading transactions are closely related to pseudonymisation data processing. On-chain crypto asset transactions, in the form of exchanges or transfers, will be recorded in the blockchain system as a wallet address or public address. In addition, physical crypto asset traders will also record and store transaction details, such as sender and recipient names, sender and recipient wallet addresses, and sender and recipient addresses, as part of their obligation to apply the travel rule principle.

Even though, in principle, the protection of pseudonymisation data requires that "additional information" that can be used to re-identify pseudonymisation data must be stored separately, physical crypto asset traders have, in practice, processed the pseudonymisation data of crypto asset customers. Unfortunately, the PDP Law does not regulate pseudonymisation data as a type subject to personal data protection principles. Moreover, physical traders of crypto assets are obligated to apply the know your customer principle.

Thus, Article 4 of the PDP Law needs to be reformed by adding "pseudonymisation data" as one type of personal data. This would give crypto asset customers legal certainty regarding legal protection in processing personal data as pseudonymisation data. Additionally, the PDP Law must accommodate criteria for re-identifying pseudonymisation data that is considered valid to guarantee legal certainty for crypto asset customers. Therefore, legal protection for crypto asset customers in processing personal data in pseudonymisation data will be achievable (not impossible) because regulations will govern it.

References

Abdul Karim, M. S., & Hadinata, F. (2023). Implikasi Filosofis Desentralisasi Bitcoin Dalam Perspektif Empire Negri-Hardt. *Jaqfi: Jurnal Aqidah dan Filsafat Islam*, *8*(1), 48–60. (In Indonesian). https://doi.org/10.15575/jaqfi.v8i1.26627

Adhiwisaksana, M. F., & Allagan, T. M. P. (2023). Competent Forum and the Applicable Law in Personal Data Protection With Foreign Element. *Indonesian Journal of International Law*, *20*(3), 442–470. https://doi.org/10.17304/ijil.vol20.3.2

Alfin, M. H., Idayanti, S., & Rahayu, K. (2024). Regulasi Dan Mekanisme Jual Beli Aset Kripto Di Indonesia. *Jurnal Ilmiah Mahasiswa Ekonomi Syariah (JIMESHA)*, *3*(2), 179–188. (In Indonesian). https://doi.org/10.36908/jimesha.v3i2.312

Anand, G., Hernoko, A. Y., & Dharmadji, A. G. (2020). The Urgency of Enacting Personal Data Protection Law As a Patronage From the Development of Communication and Information Technology in Indonesia. *Perspektif*, *25*(1), 54–62. https://doi.org/10.30742/perspektif.v25i1.750

Anggen Suari, K. R., & Sarjana, I. M. (2023). Menjaga Privasi di Era Digital: Perlindungan Data Pribadi di Indonesia. *Jurnal Analisis Hukum*, *6*(1), 132–142. (In Indonesian). https://doi.org/10.38043/jah.v6i1.4484

Asrun, A. M. (2016). Hak Asasi Manusia Dalam Kerangka Negara Hukum: Catatan Perjuangan di Mahkamah Konstitusi. *Jurnal Cita Hukum*, *4*(1), 133–154. (In Indonesian). https://doi.org/10.15408/jch.v4i1.3200

Atikah, I. (2023). Perlindungan Hukum Pelanggan Aset Kripto Transaksi Perdagangan Berjangka Komoditi Indonesia. *SALAM: Jurnal Sosial Dan Budaya Syar-I, 10*(2), 497–514. (In Indonesian). https://doi.org/10.15408/sjsbs.v10i2.31691

Ausop, A. Z., & Aulia, E. S. N. (2018). Teknologi Cryptocurrency Bitcoin Untuk Investasi Dan Transaksi Bisnis Menurut Syariat Islam. *Jurnal Sosioteknologi*, *17*(1), 74–92. (In Indonesian). https://doi.org/10.5614/sostek.itbj.2018.17.1.8

Ayunda, R. (2022). Personal Data Protection to E-Commerce Consumer: What Are the Legal Challenges and Certainties? *Law Reform*, *18*(2), 144–163. https://doi.org/10.14710/lr.v18i2.43307

Bolognini, L., & Bistolfi, C. (2017). Pseudonymization and impacts of Big (personal/anonymous) Data processing in the transition from the Directive 95/46/EC to the new EU General Data Protection Regulation. *Computer Law and Security Review*, *33*(2), 171–181. https://doi.org/10.1016/j.clsr.2016.11.002

Chang, S. E. (2019). Legal Status of Cryptocurrency in Indonesia and Legal Analysis of the Business Activities in Terms of Cryptocurrency. *Brawijaya Law Journal*, *6*(1), 76–93. https://doi.org/10.21776/ub.blj.2019.006.01.06

Dat, H. L. N. T., & An, C. T. T. (2024). The Regulation of Data Transmission in the Digital Era: From the European Union's Perspective and Implications for Vietnam. *Vietnamese Journal of Legal Sciences*, *11*(2), 1–13. https://doi.org/10.2478/vjls-2024-0007

Dewi, S. (2017). Model Regulation for Data Privacy in the Application of Biometric Smart Card. *Brawijaya Law Journal*, *4*(1), 117–128. https://doi.org/10.21776/ub.blj.2017.004.01.06

Faozi, M., & Segara Gustanto, E. (2022). Kripto, Blockchain, Bitcoin, dan Masa Depan Bank Islam: Sebuah Literatur Review. *Quranomic: Jurnal Ekonomi Dan Bisnis Islam*, *1*(2), 127–151. (In Indonesian).

Finck, M., & Pallas, F. (2020). They who must not be identified – distinguishing personal from non-personal data under the GDPR. *International Data Privacy Law*, *10*(1), 11–36. https://doi.org/10.1093/idpl/ipz026

Handoko, R. M., Aulyansyah, B., Trisna, A., & Delon, R. (2024). Implementasi Blockchain Untuk Keamanan Sistem Pembayaran Digital dan Optimasi Transaksi Keuangan (Studi Kasus Industri Fintech di Indonesia). *Teknik: Jurnal Ilmu Teknik dan Informatika*, *4*(2), 64–74. (In Indonesian).

Hintze, M., & El Emam, K. (2018). Comparing the benefits of pseudonymisation and anonymisation under the GDPR. *Journal of Data Protection and Privacy*, *2*(2), 145–158. https://doi.org/10.69554/qsst9019

Huang, T., & Zheng, S. (2023). Using Differential Privacy to Define Personal, Anonymous, and Pseudonymous Data. *IEEE Access*, *11*, 109225–109236. https://doi.org/10.1109/ACCESS.2023.3321578

Imakura, A., Sakurai, T., Okada, Y., Fujii, T., Sakamoto, T., & Abe, H. (2023). Non-readily identifiable data collaboration analysis for multiple datasets including personal information. *Information Fusion*, *98*, 101826. https://doi.org/10.1016/j.inffus.2023.101826

Jamwal, S., Cano, J., Lee, G. M., Tran, N. H., & Truong, N. (2024). A survey on Ethereum pseudonymity: Techniques, challenges, and future directions. *Journal of Network and Computer Applications*, *232*, 104019. https://doi.org/10.1016/j.jnca.2024.104019

Jati, Hardian Satria, Zulfikar, A. A. (2021). Transaksi Cryptocurrency Perspektif Hukum Ekonomi Syariah. *Al-Adalah: Jurnal Hukum Dan Politik Islam*, *6*(2), 137–148. (In Indonesian). EDN: https://elibrary.ru/mrkhni. DOI: https://doi.org/10.35673/ajmpi.v6i2.1616

Joo, M. H., & Kwon, H. Y. (2023). Comparison of personal information de-identification policies and laws within the EU, the US, Japan, and South Korea. *Government Information Quarterly*, *40*(2), 101805. https://doi.org/10.1016/j.giq.2023.101805

Jose, N. S. (2023). Information and Communication Technologies and the Right to Informational Privacy in Health Care: A Comprehensive Analysis. *Brawijaya Law Journal*, *10*(1), 34–58. https://doi.org/10.21776/ub.blj.2023.010.01.03

Kohlmayer, F., Lautenschläger, R., & Prasser, F. (2019). Pseudonymization for research data collection: Is the juice worth the squeeze? *BMC Medical Informatics and Decision Making*, *19*(1), 1–7. https://doi.org/10.1186/s12911-019-0905-x

Kumar Rai, B. (2016). Pseudonymization Techniques for Providing Privacy and Security in EHR. *International Journal of Emerging Trends & Technology in Computer Science*, *5*(4).

Limniotis, K. (2021). Cryptography as the means to protect fundamental human rights. *Cryptography*, *5*(4), 1–33. https://doi.org/10.3390/cryptography5040034

Maulana, E. T. (2024). Regulasi Travel Rule Terhadap Transaksi Aset Virtual Lintas Batas Dalam Konteks Decentralized Finance Di Indonesia: Studi Banding Terhadap Markets In Crypto-Assets (Mica) Di Uni Eropa. *JURNAL RECTUM: Tinjauan Yuridis Penanganan Tindak Pidana*, *6*(3), 565–584. (In Indonesian).

Mourby, M., Mackey, E., Elliot, M., Gowans, H., Wallace, S. E., Bell, J., Smith, H., Aidinlis, S., & Kaye, J. (2018). Are 'pseudonymised' data always personal data? Implications of the GDPR for administrative data research in the UK. *Computer Law and Security Review*, *34*(2), 222–233. https://doi.org/10.1016/j.clsr.2018.01.002

Multazam, M. T., Phahlevi, R. R., Purnomo, M. I., Purwaningsih, S. B., & Sabirov, B. (2024). Securing Blockchain Enterprises: Legal Due Diligence Amidst Rising Cyber Threats. *Padjadjaran Jurnal Ilmu Hukum (Journal of Law)*, *11*(1), 26–52. https://doi.org/10.22304/pjih.v11n1.a2

Nanda Sari, A., & Gelar, T. (2024). Blockchain: Teknologi Dan Implementasinya. *Jurnal Mnemonic*, *7*(1), 63–70. (In Indonesian). https://doi.org/10.36040/mnemonic.v7i1.6961

Pelteret, M., & Ophoff, J. (2016). A review of information privacy and its importance to consumers and organizations. *Informing Science*, *19*(1), 277–301. https://doi.org/10.28945/3573

Priliasari, E. (2023). Perlindungan Data Pribadi Konsumen Dalam Transaksi E-Commerce Menurut Peraturan Perundang-Undangan Di Indonesia (Legal Protection Of Consumer Personal Data In E-Commerce According To Laws Dan Regulations In Indonesia). *Jurnal Rechts Vinding*, *12*(2), 261–279. (In Indonesian).

Priskarini, I. A., Pranoto, & Tejomurti, K. (2019). The Role of The Financial Services Authority in The Legal Protection of Privacy Rights in Connection with Personal Data of Fintech Lending Debtor in Indonesia. *Padjadjaran Jurnal Ilmu Hukum (Journal of Law)*, *6*(3), 556–575. https://doi.org/10.22304/pjih.v6n3.a7

Pudjastuti, K. G., & Westra, I. K. (2021). Legalitas Mata Uang Virtual Bitcoin Dalam Transaksi Online Di Indonesia. *Kertha Wicara: Journal Ilmu Hukum*, *9*(11), 1–10. (In Indonesian).

Rizko Ramadoni, S., Sukarmi, S., & Nur Widhiyanti, H. (2021). Konvergensi Hukum Penentuan Suku Bunga dalam Layanan Pinjam Meminjam Uang Berbasis Teknologi Informasi. *Jurnal Magister Hukum Udayana (Udayana Master Law Journal)*, *9*(4), 821–837. (In Indonesian). https://doi.org/10.24843/jmhu.2020.v09.i04.p11

Rohmansyah, D. A., Saputra, K. M., & Sholih, B. (2023). Urgensi Perlindungan Hak Asasi Anak Atas Data Pribadi di Era Digitilasasi Berdasarkan Prinsip Negara Hukum. *AL-MANHAJ: Jurnal Hukum Dan Pranata Sosial Islam*, *5*(2), 1099–1110. (In Indonesian). https://doi.org/10.37680/almanhaj.v5i2.3054

Setiawan, R. C., Idayanti, S., & Wildan, M. (2023). Perkembangan Komoditi Digital Dalam Aset Kripto Di Indonesia. *Pancasakti Law Journal*, *1*(2), 369–384. (In Indonesian).

Sinaga, E. M. C., & Putri, M. Ch. (2020). Formulasi Legislasi Perlindungan Data Pribadi Dalam Revolusi Industri 4.0. *Rechts Vinding: Media Pembinaan Hukum Nasional*, *9*(2), 237–256. (In Indonesian). https://doi.org/10.33331/rechtsvinding.v9i2.428

Sinulingga, D. A. (2022). Legal Certainty of Aggregate Data Utilization in The Design of Personal Data Protection Bill. *Jambura Law Review*, *4*(1), 18–37. https://doi.org/10.33756/jlr.v4i1.11973

Soraja, A. (2021). Perlindungan Hukum Atas Hak Privasi Dan Data Pribadi Dalam Perspektif Ham. *Seminar Nasional – Kota Ramah Hak Asasi Manusia*, *1*, 20–32. (In Indonesian).

Štarchoň, P., & Pikulík, T. (2019). GDPR principles in data protection encourage pseudonymization through most popular and full-personalized devices – mobile phones. *Procedia Computer Science*, *151*(2018), 303–312. https://doi.org/10.1016/j.procs.2019.04.043

Suryawijaya, T. W. E. (2023). Memperkuat Keamanan Data melalui Teknologi Blockchain: Mengeksplorasi Implementasi Sukses dalam Transformasi Digital di Indonesia. *Jurnal Studi Kebijakan Publik*, *2*(1), 55–68. (In Indonesian). https://doi.org/10.21787/jskp.2.2023.55-68

Syailendra, M. R., Lie, G., & Sudiro, A. (2024). Personal Data Protection Law in Indonesia: Challenges and Opportunities. *Indonesia Law Review*, *14*(2), 56–72.

Tatar, U., Gokce, Y., & Nussbaum, B. (2020). Law versus technology: Blockchain, GDPR, and tough tradeoffs. *Computer Law and Security Review*, *38*, 105454. https://doi.org/10.1016/j.clsr.2020.105454

Tirtakoesoemah, A. J., & Arafat, M. R. (2019). Penerapan Teori Perlindungan Hukum Terhadap Hak Cipta Atas Penyiaran. *Pena Justisia*, *18*(1), 1–14. (In Indonesian). https://doi.org/10.31941/pj.v18i1.1084

Ulya, W., & Pambudi, L. A. (2024). Analisis Kebijakan Cryptocurrency dalam Perspektif Sadd Al-Dzari'ah. *Jurnal Al Azhar Indonesia Seri Ilmu Sosial*, *5*(2), 102–111. (In Indonesian).

Utomo, T. P. (2022). Implementasi Teknologi Blockchain Di Perpustakaan: Peluang, Tantangan Dan Hambatan. *Buletin Perpustakaan*, *4*(2), 173–200. (In Indonesian).

Utomo, Y. A. (2020). Legal Protection for Problem Debtor Related to the Use of the Artificial Intelligence System in Peer to Peer Lending. *Yuridika*, *35*(3), 657. https://doi.org/10.20473/ydk.v35i3.19007

Wahyuningtyas, S. Yu. (2024). Legal Issues of Online Reputation Portability in the Digital Economy. *Jurnal Perkotaan*, *15*(2), 63–81. https://doi.org/10.25170/perkotaan.v15i2.5670

Yetno, A. (2021). Perlindungan Data Pribadi Dengan Prinsip Mengutamakan Melindungi Privasi Pengguna Dalam Upaya Mewujudkan Tujuan Hukum Di Indonesia. *Satya Dharma: Journal Ilmu Hukum*, *4*(1). (In Indonesian).

Authors information

Mayuna I Komang Oki – Master of Law Student, Faculty of Law, Brawijaya University
Address: MT. Haryono St 169, Malang City, East Java Province, Indonesia, 65145
E-mail: okimayuna04@student.ub.ac.id
ORCID ID: https://orcid.org/0009-0002-0016-4788
Google Scholar ID: https://scholar.google.com/citations?user=H4cIKpwAAAAJ

Dewantara Reka – Dr. (Law), Associate Professor, Faculty of Law, Brawijaya University
Address: MT. Haryono St 169, Malang City, East Java Province, Indonesia, 65145
E-mail: rainerfh@ub.ac.id
ORCID ID: https://orcid.org/0000-0002-6010-0279
Scopus Author ID: https://www.scopus.com/authid/detail.uri?authorId=58317982600
Google Scholar ID: https://scholar.google.co.id/citations?user=kP38YuQAAAAJ

Ruslijanto Patricia Audrey – Dr. (Law), Associate Professor, Faculty of Law, Brawijaya University
Address: MT. Haryono St 169, Malang City, East Java Province, Indonesia, 65145
E-mail: patricia@ub.ac.id
ORCID ID: https://orcid.org/0009-0006-6621-832X
Scopus Author ID: https://www.scopus.com/authid/detail.uri?authorId=57201777768
Google Scholar ID: https://scholar.google.com/citations?user=TSr2eYoAAAAJ

Authors' contributions

The authors have contributed equally into the concept and methodology elaboration, validation, formal analysis, research, selection of sources, text writing and editing, project guidance and management.

Conflict of interest

The authors declares no conflict of interest.

Financial disclosure

The research had no sponsorship.

Thematic rubrics

OECD: 5.05 / Law
PASJC: 3308 / Law
WoS: OM / Law

Article history

Date of receipt – February 21, 2025
Date of approval – March 15, 2025
Date of acceptance – June 20, 2025
Date of online placement – June 25, 2025

Научная статья
УДК 34:004:346.6:004.7
EDN: https://elibrary.ru/lqycmn
DOI: https://doi.org/10.21202/jdtl.2025.12

Псевдонимизация персональных данных пользователей криптоактивов: проблемы правового регулирования в Индонезии

И Команг Оки Маюна ✉
Университет Бравиджая, Маланг, Индонезия

Река Девантара
Университет Бравиджая, Маланг, Индонезия

Патриция Одри Руслиджанто
Университет Бравиджая, Маланг, Индонезия

Ключевые слова

законодательство,
защита персональных данных,
криптоактивы,
криптовалюта,
персональные данные,
право,
псевдонимизация,
технология блокчейн,
торговля криптоактивами,
цифровые технологии

Аннотация

Цель: анализ возможности обеспечения правовой защиты псевдонимизированных персональных данных пользователей криптоактивов в правовой системе Индонезии.

Методы: в работе применяется комплексный правовой анализ, основанный на изучении действующих нормативных правовых актов Индонезии в сфере защиты персональных данных. Исследование реализовано с использованием законодательного, концептуального и сравнительного методологических подходов, включающих анализ положений индонезийского Закона о защите персональных данных, Общего регламента Европейского союза по защите персональных данных и британского Закона о защите данных.

Результаты: установлено, что псевдонимизация данных пользователей криптоактивов в Индонезии осуществима с правовой точки зрения, однако существующее законодательство содержит существенные пробелы. Действующий Закон о защите персональных данных Индонезии не признает псевдонимизированные данные в качестве отдельной категории персональных данных, подлежащих правовой защите. Выявлена проблематичность реализации правила контроля переводов физическими трейдерами криптоактивов, поскольку дополнительная информация для реидентификации псевдонимизированных данных не хранится отдельно, что увеличивает риски нарушения конфиденциальности.

✉ Корреспондирующий автор

Научная новизна: проведен комплексный анализ правовых механизмов защиты псевдонимизированных данных в контексте криптовалютных операций. Предложена концептуальная модель совершенствования национального законодательства о защите персональных данных путем включения псевдонимизированных данных в качестве отдельной категории защищаемой информации. Разработаны рекомендации по установлению критериев законной реидентификации псевдонимизированных данных для обеспечения правовой определенности в сфере защиты пользователей криптоактивов.

Практическая значимость: результаты исследования могут служить теоретико-методологической основой для реформирования индонезийского Закона о защите персональных данных и создания эффективного правового механизма защиты пользователей криптоактивов. Предложенные изменения в ст. 4 указанного Закона позволят включить псевдонимизированные данные в перечень защищаемых категорий персональных данных, что обеспечит правовую определенность для участников криптовалютного рынка и повысит уровень защиты их персональных данных в условиях цифровой экономики.

Для цитирования

Маюна, И К. О., Девантара, Р., Руслиджанто, П. О. (2025). Псевдонимизация персональных данных пользователей криптоактивов: проблемы правового регулирования в Индонезии. *Journal of Digital Technologies and Law*, *3*(2), 275–303. https://doi.org/10.21202/jdtl.2025.12

Список литературы

Abdul Karim, M. S., & Hadinata, F. (2023). Implikasi Filosofis Desentralisasi Bitcoin Dalam Perspektif Empire Negri-Hardt. *Jaqfi: Jurnal Aqidah dan Filsafat Islam*, *8*(1), 48–60. (In Indonesian). https://doi.org/10.15575/jaqfi.v8i1.26627

Adhiwisaksana, M. F., & Allagan, T. M. P. (2023). Competent Forum and the Applicable Law in Personal Data Protection With Foreign Element. *Indonesian Journal of International Law*, *20*(3), 442–470. https://doi.org/10.17304/ijil.vol20.3.2

Alfin, M. H., Idayanti, S., & Rahayu, K. (2024). Regulasi Dan Mekanisme Jual Beli Aset Kripto Di Indonesia. *Jurnal Ilmiah Mahasiswa Ekonomi Syariah (JIMESHA)*, *3*(2), 179–188. (In Indonesian). https://doi.org/10.36908/jimesha.v3i2.312

Anand, G., Hernoko, A. Y., & Dharmadji, A. G. (2020). The Urgency of Enacting Personal Data Protection Law As a Patronage From the Development of Communication and Information Technology in Indonesia. *Perspektif*, *25*(1), 54–62. https://doi.org/10.30742/perspektif.v25i1.750

Anggen Suari, K. R., & Sarjana, I. M. (2023). Menjaga Privasi di Era Digital: Perlindungan Data Pribadi di Indonesia. *Jurnal Analisis Hukum*, *6*(1), 132–142. (In Indonesian). https://doi.org/10.38043/jah.v6i1.4484

Asrun, A. M. (2016). Hak Asasi Manusia Dalam Kerangka Negara Hukum: Catatan Perjuangan di Mahkamah Konstitusi. *Jurnal Cita Hukum*, *4*(1), 133–154. (In Indonesian). https://doi.org/10.15408/jch.v4i1.3200

Atikah, I. (2023). Perlindungan Hukum Pelanggan Aset Kripto Transaksi Perdagangan Berjangka Komoditi Indonesia. *SALAM: Jurnal Sosial Dan Budaya Syar-I, 10*(2), 497–514. (In Indonesian). https://doi.org/10.15408/sjsbs.v10i2.31691

Ausop, A. Z., & Aulia, E. S. N. (2018). Teknologi Cryptocurrency Bitcoin Untuk Investasi Dan Transaksi Bisnis Menurut Syariat Islam. *Jurnal Sosioteknologi*, *17*(1), 74–92. (In Indonesian). https://doi.org/10.5614/sostek.itbj.2018.17.1.8

Ayunda, R. (2022). Personal Data Protection to E-Commerce Consumer: What Are the Legal Challenges and Certainties? *Law Reform*, *18*(2), 144–163. https://doi.org/10.14710/lr.v18i2.43307

Bolognini, L., & Bistolfi, C. (2017). Pseudonymization and impacts of Big (personal/anonymous) Data processing in the transition from the Directive 95/46/EC to the new EU General Data Protection Regulation. *Computer Law and Security Review*, *33*(2), 171–181. https://doi.org/10.1016/j.clsr.2016.11.002

Chang, S. E. (2019). Legal Status of Cryptocurrency in Indonesia and Legal Analysis of the Business Activities in Terms of Cryptocurrency. *Brawijaya Law Journal*, *6*(1), 76–93. https://doi.org/10.21776/ub.blj.2019.006.01.06

Dat, H. L. N. T., & An, C. T. T. (2024). The Regulation of Data Transmission in the Digital Era: From the European Union's Perspective and Implications for Vietnam. *Vietnamese Journal of Legal Sciences*, *11*(2), 1–13. https://doi.org/10.2478/vjls-2024-0007

Dewi, S. (2017). Model Regulation for Data Privacy in the Application of Biometric Smart Card. *Brawijaya Law Journal*, *4*(1), 117–128. https://doi.org/10.21776/ub.blj.2017.004.01.06

Faozi, M., & Segara Gustanto, E. (2022). Kripto, Blockchain, Bitcoin, dan Masa Depan Bank Islam: Sebuah Literatur Review. *Quranomic: Jurnal Ekonomi Dan Bisnis Islam*, *1*(2), 127–151. (In Indonesian).

Finck, M., & Pallas, F. (2020). They who must not be identified – distinguishing personal from non-personal data under the GDPR. *International Data Privacy Law*, *10*(1), 11–36. https://doi.org/10.1093/idpl/ipz026

Handoko, R. M., Aulyansyah, B., Trisna, A., & Delon, R. (2024). Implementasi Blockchain Untuk Keamanan Sistem Pembayaran Digital dan Optimasi Transaksi Keuangan (Studi Kasus Industri Fintech di Indonesia). *Teknik: Jurnal Ilmu Teknik dan Informatika*, *4*(2), 64–74. (In Indonesian).

Hintze, M., & El Emam, K. (2018). Comparing the benefits of pseudonymisation and anonymisation under the GDPR. *Journal of Data Protection and Privacy*, *2*(2), 145–158. https://doi.org/10.69554/qsst9019

Huang, T., & Zheng, S. (2023). Using Differential Privacy to Define Personal, Anonymous, and Pseudonymous Data. *IEEE Access*, *11*, 109225–109236. https://doi.org/10.1109/ACCESS.2023.3321578

Imakura, A., Sakurai, T., Okada, Y., Fujii, T., Sakamoto, T., & Abe, H. (2023). Non-readily identifiable data collaboration analysis for multiple datasets including personal information. *Information Fusion*, *98*, 101826. https://doi.org/10.1016/j.inffus.2023.101826

Jamwal, S., Cano, J., Lee, G. M., Tran, N. H., & Truong, N. (2024). A survey on Ethereum pseudonymity: Techniques, challenges, and future directions. *Journal of Network and Computer Applications*, *232*, 104019. https://doi.org/10.1016/j.jnca.2024.104019

Jati, Hardian Satria, Zulfikar, A. A. (2021). Transaksi Cryptocurrency Perspektif Hukum Ekonomi Syariah. *Al-Adalah: Jurnal Hukum Dan Politik Islam*, *6*(2), 137–148. (In Indonesian). EDN: https://elibrary.ru/mrkhni. DOI: https://doi.org/10.35673/ajmpi.v6i2.1616

Joo, M. H., & Kwon, H. Y. (2023). Comparison of personal information de-identification policies and laws within the EU, the US, Japan, and South Korea. *Government Information Quarterly*, *40*(2), 101805. https://doi.org/10.1016/j.giq.2023.101805

Jose, N. S. (2023). Information and Communication Technologies and the Right to Informational Privacy in Health Care: A Comprehensive Analysis. *Brawijaya Law Journal*, *10*(1), 34–58. https://doi.org/10.21776/ub.blj.2023.010.01.03

Kohlmayer, F., Lautenschläger, R., & Prasser, F. (2019). Pseudonymization for research data collection: Is the juice worth the squeeze? *BMC Medical Informatics and Decision Making*, *19*(1), 1–7. https://doi.org/10.1186/s12911-019-0905-x

Kumar Rai, B. (2016). Pseudonymization Techniques for Providing Privacy and Security in EHR. *International Journal of Emerging Trends & Technology in Computer Science*, *5*(4).

Limniotis, K. (2021). Cryptography as the means to protect fundamental human rights. *Cryptography*, *5*(4), 1–33. https://doi.org/10.3390/cryptography5040034

Maulana, E. T. (2024). Regulasi Travel Rule Terhadap Transaksi Aset Virtual Lintas Batas Dalam Konteks Decentralized Finance Di Indonesia: Studi Banding Terhadap Markets In Crypto-Assets (Mica) Di Uni Eropa. *JURNAL RECTUM: Tinjauan Yuridis Penanganan Tindak Pidana*, *6*(3), 565–584. (In Indonesian).

Mourby, M., Mackey, E., Elliot, M., Gowans, H., Wallace, S. E., Bell, J., Smith, H., Aidinlis, S., & Kaye, J. (2018). Are 'pseudonymised' data always personal data? Implications of the GDPR for administrative data research in the UK. *Computer Law and Security Review*, *34*(2), 222–233. https://doi.org/10.1016/j.clsr.2018.01.002

Multazam, M. T., Phahlevi, R. R., Purnomo, M. I., Purwaningsih, S. B., & Sabirov, B. (2024). Securing Blockchain Enterprises: Legal Due Diligence Amidst Rising Cyber Threats. *Padjadjaran Jurnal Ilmu Hukum (Journal of Law)*, *11*(1), 26–52. https://doi.org/10.22304/pjih.v11n1.a2

Nanda Sari, A., & Gelar, T. (2024). Blockchain: Teknologi Dan Implementasinya. *Jurnal Mnemonic*, *7*(1), 63–70. (In Indonesian). https://doi.org/10.36040/mnemonic.v7i1.6961

Pelteret, M., & Ophoff, J. (2016). A review of information privacy and its importance to consumers and organizations. *Informing Science*, *19*(1), 277–301. https://doi.org/10.28945/3573

Priliasari, E. (2023). Perlindungan Data Pribadi Konsumen Dalam Transaksi E-Commerce Menurut Peraturan Perundang-Undangan Di Indonesia (Legal Protection Of Consumer Personal Data In E-Commerce According To Laws Dan Regulations In Indonesia). *Jurnal Rechts Vinding*, *12*(2), 261–279. (In Indonesian).

Priskarini, I. A., Pranoto, & Tejomurti, K. (2019). The Role of The Financial Services Authority in The Legal Protection of Privacy Rights in Connection with Personal Data of Fintech Lending Debtor in Indonesia. *Padjadjaran Jurnal Ilmu Hukum (Journal of Law)*, *6*(3), 556–575. https://doi.org/10.22304/pjih.v6n3.a7

Pudjastuti, K. G., & Westra, I. K. (2021). Legalitas Mata Uang Virtual Bitcoin Dalam Transaksi Online Di Indonesia. *Kertha Wicara: Journal Ilmu Hukum*, *9*(11), 1–10. (In Indonesian).

Rizko Ramadoni, S., Sukarmi, S., & Nur Widhiyanti, H. (2021). Konvergensi Hukum Penentuan Suku Bunga dalam Layanan Pinjam Meminjam Uang Berbasis Teknologi Informasi. *Jurnal Magister Hukum Udayana (Udayana Master Law Journal)*, *9*(4), 821–837. (In Indonesian). https://doi.org/10.24843/jmhu.2020.v09.i04.p11

Rohmansyah, D. A., Saputra, K. M., & Sholih, B. (2023). Urgensi Perlindungan Hak Asasi Anak Atas Data Pribadi di Era Digitilasasi Berdasarkan Prinsip Negara Hukum. *AL-MANHAJ: Jurnal Hukum Dan Pranata Sosial Islam*, *5*(2), 1099–1110. (In Indonesian).

Setiawan, R. C., Idayanti, S., & Wildan, M. (2023). Perkembangan Komoditi Digital Dalam Aset Kripto Di Indonesia. *Pancasakti Law Journal*, *1*(2), 369–384. (In Indonesian). https://doi.org/10.24905/plj.v1i2.32

Sinaga, E. M. C., & Putri, M. Ch. (2020). Formulasi Legislasi Perlindungan Data Pribadi Dalam Revolusi Industri 4.0. *Rechts Vinding: Media Pembinaan Hukum Nasional*, *9*(2), 237–256. (In Indonesian). https://doi.org/10.33331/rechtsvinding.v9i2.428

Sinulingga, D. A. (2022). Legal Certainty of Aggregate Data Utilization in The Design of Personal Data Protection Bill. *Jambura Law Review*, *4*(1), 18–37. https://doi.org/10.33756/jlr.v4i1.11973

Soraja, A. (2021). Perlindungan Hukum Atas Hak Privasi Dan Data Pribadi Dalam Perspektif Ham. *Seminar Nasional – Kota Ramah Hak Asasi Manusia*, *1*, 20–32. (In Indonesian).

Štarchoň, P., & Pikulík, T. (2019). GDPR principles in data protection encourage pseudonymization through most popular and full-personalized devices – mobile phones. *Procedia Computer Science*, *151*(2018), 303–312. https://doi.org/10.1016/j.procs.2019.04.043

Suryawijaya, T. W. E. (2023). Memperkuat Keamanan Data melalui Teknologi Blockchain: Mengeksplorasi Implementasi Sukses dalam Transformasi Digital di Indonesia. *Jurnal Studi Kebijakan Publik*, *2*(1), 55–68. (In Indonesian). https://doi.org/10.21787/jskp.2.2023.55-68

Syailendra, M. R., Lie, G., & Sudiro, A. (2024). Personal Data Protection Law in Indonesia: Challenges and Opportunities. *Indonesia Law Review*, *14*(2), 56–72.

Tatar, U., Gokce, Y., & Nussbaum, B. (2020). Law versus technology: Blockchain, GDPR, and tough tradeoffs. *Computer Law and Security Review*, *38*, 105454. https://doi.org/10.1016/j.clsr.2020.105454

Tirtakoesoemah, A. J., & Arafat, M. R. (2019). Penerapan Teori Perlindungan Hukum Terhadap Hak Cipta Atas Penyiaran. *Pena Justisia*, *18*(1), 1–14. (In Indonesian). https://doi.org/10.31941/pj.v18i1.1084

Ulya, W., & Pambudi, L. A. (2024). Analisis Kebijakan Cryptocurrency dalam Perspektif Sadd Al-Dzari'ah. *Jurnal Al Azhar Indonesia Seri Ilmu Sosial*, *5*(2), 102–111. (In Indonesian).

Utomo, T. P. (2022). Implementasi Teknologi Blockchain Di Perpustakaan: Peluang, Tantangan Dan Hambatan. *Buletin Perpustakaan*, *4*(2), 173–200. (In Indonesian).

Utomo, Y. A. (2020). Legal Protection for Problem Debtor Related to the Use of the Artificial Intelligence System in Peer to Peer Lending. *Yuridika*, *35*(3), 657. https://doi.org/10.20473/ydk.v35i3.19007

Wahyuningtyas, S. Yu. (2024). Legal Issues of Online Reputation Portability in the Digital Economy. *Jurnal Perkotaan*, *15*(2), 63–81. https://doi.org/10.25170/perkotaan.v15i2.5670

Yetno, A. (2021). Perlindungan Data Pribadi Dengan Prinsip Mengutamakan Melindungi Privasi Pengguna Dalam Upaya Mewujudkan Tujuan Hukum Di Indonesia. *Satya Dharma: Journal Ilmu Hukum*, *4*(1). (In Indonesian).

Сведения об авторах

Маюна И Команг Оки – магистрант в области права, факультет права, Университет Бравиджая
Адрес: Индонезия, 65145, провинция Западной Явы, г. Маланг, ул. МТ. Арьоно, д. 169
E-mail: okimayuna04@student.ub.ac.id
ORCID ID: https://orcid.org/0009-0002-0016-4788
Google Scholar ID: https://scholar.google.com/citations?user=H4clKpwAAAAJ

Девантара Река – доктор права, доцент, факультет права, Университет Бравиджая
Адрес: Индонезия, 65145, провинция Западной Явы, г. Маланг, ул. МТ. Арьоно, д. 169
E-mail: rainerfh@ub.ac.id
ORCID ID: https://orcid.org/0000-0002-6010-0279
Scopus Author ID: https://www.scopus.com/authid/detail.uri?authorId=58317982600
Google Scholar ID: https://scholar.google.co.id/citations?user=kP38YuQAAAAJ

Руслиджанто Патриция Одри – доктор права, доцент, факультет права, Университет Бравиджая
Адрес: Индонезия, 65145, провинция Западной Явы, г. Маланг, ул. МТ. Арьоно, д. 169
E-mail: patricia@ub.ac.id
ORCID ID: https://orcid.org/0009-0006-6621-832X
Scopus Author ID: https://www.scopus.com/authid/detail.uri?authorId=57201777768
Google Scholar ID: https://scholar.google.com/citations?user=TSr2eYoAAAAJ

Вклад авторов

Авторы внесли равный вклад в разработку концепции, методологии, валидацию, формальный анализ, проведение исследования, подбор источников, написание и редактирование текста, руководство и управление проектом.

Конфликт интересов

Авторы сообщают об отсутствии конфликта интересов.

Финансирование

Исследование не имело спонсорской поддержки.

Тематические рубрики

Рубрика OECD: 5.05 / Law
Рубрика ASJC: 3308 / Law
Рубрика WoS: OM / Law
Рубрика ГРНТИ: 10.19.31 / Право на информацию
Специальность ВАК: 5.1.3 / Частно-правовые (цивилистические) науки

История статьи

Дата поступления – 21 февраля 2025 г.
Дата одобрения после рецензирования – 15 марта 2025 г.
Дата принятия к опубликованию – 20 июня 2025 г.
Дата онлайн-размещения – 25 июня 2025 г.