Account Blocking Without Customer Consent: Disharmony Between The Banking Law, The PDP Law, and POJK 8/2023

Yulius Ariyasatya[1*], Luthy Yustika[2]

[1,2] Faculty of Law, Esa Unggul University, Jakarta, Indonesia
*Corresponding Author:
Email:Yulius.ariyasatya@gmail.com

Abstract

Banks blocking customer accounts without consent or notification raises legal issues related to customer protection and data privacy. Under the framework of Law No. 7/1992 in conjunction with Law No. 10/1998, such actions can be justified as an exception if based on orders from law enforcement officials. However, following the enactment of POJK No. 22/2023 concerning Consumer Protection in the Financial Services Sector and Law No. 27/2022 concerning Personal Data Protection, the practice of blocking accounts without customer consent has the potential to conflict with the principles of transparency, accountability, and control of personal data by banks. This study normatively analyzes the potential for disharmony between regulations through a review of laws and regulations, legal literature, and banking practices, using the Theory of Legal Protection and the Theory of Presumption of Innocence as analytical tools. The study's findings demonstrate the need for adequate consent and notification in any action that impacts customer rights, as well as strengthening operational harmonization and oversight so that blocking procedures do not violate privacy rights or legal certainty. Recommendations include the development of clear operational standards, transparency of processes, and accountability of banks as data controllers, so that customer legal protection is optimally achieved.

Keywords: *Presumption of Innocence; Consumer Protection; Personal Data Protection; Transparency; Accountability; Regulatory Harmonization and Banking.*

I. INTRODUCTION

The development of digitalization in the Indonesian banking sector has transformed services and expanded the scope of regulation. The integration of information technology has increased the efficiency of customer data management and financial transactions, but simultaneously presents new challenges related to the fulfillment of customer rights and the protection of personal data. One prominent issue is the practice of blocking accounts without adequate consent or notification. This action is typically carried out at the request of law enforcement officials or to prevent money laundering, but it still raises legal questions regarding its coherence with banking law and consumer protection principles.Normatively, account data is considered personal data under Law Number 27 of 2022 concerning Personal Data Protection (PDP Law). The PDP Law emphasizes that personal data is a constitutional right that must be kept confidential and that data processing can only be carried out with the data subject's consent. This provision aligns with Article 28G of the 1945 Constitution, which guarantees personal protection and the right to privacy for every citizen (Sholat and Apriandani, 2024). Therefore, blocking an account without consent potentially violates the principles of the presumption of innocence, equality before the law, and the principles of personal data protection and confidentiality.On the other hand, the Financial Services Authority (OJK) through POJK No. 8 of 2023 emphasizes the urgency of transparency, accountability, and customer consent for any actions that impact customer rights (Sembiring and Hum, 2024).

This regulation is also aimed at strengthening the Anti-Money Laundering (AML, CFT) and Anti-Money Laundering (PPPSPM) programs by maintaining a balance between law enforcement and consumer protection. However, empirical practice shows gaps, such as the blocking of dormant accounts without prior notification to customers.This situation underscores the need for an in-depth legal study to assess the scope of legal justification for blocking without consent, as well as to formulate a harmonization between the PDP Law, the Banking Law, the Consumer Protection Law, and POJK 8/2023. This research is expected to provide a scientific contribution to regulatory alignment, ensuring the effective application of prudential principles in the financial services sector without neglecting customer rights as legal subjects.Based on this

background, the formulation of this problem is divided into two, namely: (1) What is the legal review of blocking accounts without customer consent based on POJK 8/2023? and (2) How are legal policies related to blocking accounts updated from the perspective of banking law and personal data protection in the future?

II. METHODS

This research uses a normative legal approach (Dr. Gunardi, 2022), focusing on the study of applicable legal norms. The primary objective is to gain a comprehensive understanding of the regulation of account blocking without customer consent, particularly in the context of POJK 8/2023 concerning the implementation of AML, PPT, and PPPSPM, along with its relationship to banking law and personal data protection.The approach used is a statute approach, by examining relevant laws and regulations, legal doctrine, and court decisions (Dr. Muhaimin, 2020). The sources of legal materials include: Pancasila; the 1945 Constitution; the Criminal Code; Banking Law No. 7 of 1992 in conjunction with Law No. 10 of 1998; Law No. 8 of 2010; Law No. 27 of 2022; Law No. 4 of 2023 (P2SK); and POJK No. 8 of 2023 concerning the implementation of APU PPT PPPSPM in the financial services sector.The legal material was collected through a literature review, examining legal documents, academic literature, and relevant regulations. The analysis employed a qualitative legal method, interpreting legal provisions and linking them to the research issue to obtain a comprehensive picture of the suitability of account blocking practices to banking law principles and personal data protection.

Overall, this study aims to analyze the legal aspects of account blocking without consent based on POJK 8/2023 and related regulations, and assess policy reform options from the perspective of banking law and personal data protection. The research benefits include theoretical benefits (contributions to the development of legal science and enrichment of the literature on regulatory harmonization) and practical benefits (input for regulators; guidelines for banks in formulating transparent, accountable, and prudential procedures; and education for the public regarding the rights to personal data protection and account blocking procedures). Ultimately, the recommendations are expected to support the effectiveness of the blocking mechanism while ensuring legal certainty and human rights protection. This research relies on two fundamental principles as analytical tools: the Principle of Legal Protection and the Presumption of Innocence. Both serve as foundations for assessing the practice of blocking customer accounts and protecting individual rights as legal subjects.

1. Principle of Legal Protection

The implementation of the principle of legal protection in Indonesia still faces several obstacles, such as pressure from public opinion, social stigma, and media influence, which can affect the objectivity of law enforcement officials. Protection for suspects or defendants includes the right to privacy, security guarantees, and protection from social and administrative sanctions before valid evidence is presented in court. This principle affirms that every citizen has the right to legal protection without discrimination based on social, economic, or other background status. In the context of personal data protection, this principle ensures equal protection of individual data, including the right to privacy and the right to defend themselves (Siagian & Dompak, n.d.). More broadly, human rights (HAM) are the basis for guaranteeing the protection of personal data, as data misuse has the potential to impact access to public services, economic opportunities, and social standing (Angraini et al., 2024).

The normative framework is reinforced by Law No. 27 of 2022 concerning Personal Data Protection, which positions banks as Personal Data Controllers with an obligation to maintain the security, confidentiality, and integrity of customer data. Similarly, POJK No. 8 of 2023 emphasizes the principles of transparency and accountability to protect customer legal rights, including in the implementation of the Anti-Money Laundering (AML, CFT) and Anti-Money Laundering (PPPSPM) programs.As formulated by Philipus M. Hadjon in his classic work, legal protection against government action includes preventive and repressive mechanisms (Hadjon, 1987). Preventive protection is provided before a dispute arises through the opportunity to file objections, obtain information, and express opinions. Repressive protection, on the other hand, is provided after the dispute has been resolved through the courts, including the awarding of compensation or restoration of rights.

2. Principle of Presumption of Innocence (Presumption of Innocence)

This principle is rooted in the thinking of classical figures such as Cesare Beccaria, Montesquieu, and Voltaire. In Dei delitti e delle pene, Beccaria asserted that a person should not be treated as guilty before a final and binding court decision; punishment before a verdict is categorized as an arbitrary act of the state (Beccaria, 1764/1986). Montesquieu, through L'Esprit des lois, emphasized the separation of powers (trias politica) as an institutional prerequisite for the effective implementation of the presumption of innocence (Montesquieu, 1748/1989). Voltaire contributed to the idea of fair trial, the prevention of wrongful arrest, and the strengthening of the defendant's right to defense (Voltaire, 1766/2005).Normatively, the presumption of innocence requires that any individual suspected of committing a crime be presumed innocent until a final and binding court decision is issued (Doodoh & Tuwaidan, 2025). In banking and consumer protection practices, this principle is relevant because account blocking is often based on suspected customer involvement in a crime before a final court decision is issued (Aprilia et al., 2025).

III. RESULT AND DISCUSSION

Legal Review of Account Blocking without Customer Consent under POJK 8/2023

In Law Number 10 of 1998 concerning Banking (hereinafter referred to as the Banking Law), a bank is defined as a business entity that collects funds from the public in the form of deposits and distributes them back to the public in the form of credit and/or other financing instruments to improve the public's standard of living. Customers are understood as those who utilize bank services.Ownership of savings/accounts is proven through, among other things, customer data, including the account number in the customer's name. This information is obtained upon account opening, when the bank asks prospective customers to fill out a personal data form and submit identification documents, such as an Identity Card (KTP) and Taxpayer Identification Number (NPWP). For legal entities, banks require a Deed of Establishment, the company's NPWP, and supporting documents confirming its legal entity status. When granting credit, banks may also require collateral or proof of ownership, such as a land title certificate, proof of PBB payment, vehicle registration certificate (BPKB), and other relevant documents as needed for risk assessment.All personal and legal entity data collected constitutes customer data, the confidentiality of which must be protected by banks. Article 40 of the Banking Law affirms banks' obligation to maintain confidentiality regarding customer information and their deposits. Exceptions to the disclosure of bank confidentiality are regulated in Articles 41 to 48 of the Banking Law, which essentially permit the disclosure of information for tax purposes, settlement of bank receivables, criminal justice, and the exchange of information between banks. Outside the scope of these exceptions, disclosure of customer data requires the customer's consent.

Violation of the obligation to maintain confidentiality of customer data carries criminal consequences. Article 47A of the Banking Law stipulates a minimum prison sentence of 2 (two) years and a maximum of 7 (seven) years, and a fine of at least IDR 4 billion and a maximum of IDR 15 billion. Furthermore, failure to comply with the obligation to provide mandatory information as stipulated in Article 48 of the Banking Law is punishable by a minimum prison sentence of 2 (two) years and a maximum of 10 (ten) years, with a minimum fine of IDR 5 billion and a maximum of IDR 100 billion. In addition to criminal sanctions, banks may be subject to administrative sanctions and civil liability (compensation) for losses incurred.Within the framework of POJK 8/2023, the obligations of transparency, accountability, and compliance in the AML, PPT, and PPPSPM program must be implemented without neglecting the bank secrecy regime as stipulated in the Banking Law. Therefore, blocking an account without customer consent must be supported by a clear legal basis (for example, an official request from law enforcement in a criminal case) and implemented according to documented procedures to ensure it does not conflict with customer data protection and does not incur criminal or administrative liability for the bank.A number of legal provisions outlined above provide justification for disclosing customer data, which is fundamentally protected by the banking secrecy regime. Regarding account blocking, the Banking Law (Law No. 10 of 1998) does not contain an explicit definition or specific article directly describing the act of "blocking an account." In principle, the Banking Law upholds the fiduciary principle and confidentiality, so restricting access to an account can only be justified if it is based on a valid legal basis and a measurable interest.

A. Conditions that Justify Account Blocking

Account blocking can be carried out legally if there is a statutory order or an order from an authorized official, including within the framework of:

1. The process of investigating criminal acts according to the Criminal Procedure Code,
2. Money laundering (TPPU), terrorism financing,
3. Taxation, bankruptcy, or court orders (seizure orders and execution of judgments).

In practice, blocking for law enforcement purposes is usually carried out at the official request of law enforcement officials (the National Police, the Prosecutor's Office, the Courts, or the Corruption Eradication Commission). Outside of criminal contexts, blocking can be based on clauses in the agreement between the bank and the customer, for example: an inactive (dormant) account, indications of misuse, or violations of the terms and conditions of banking services.

B. Normative Dilemmas and Customer Rights

Although blocking is often intended for law enforcement purposes, money laundering prevention, or financial system protection, this action presents a dilemma: on the one hand, banks are obligated to support system integrity; on the other, restricting access to accounts potentially violates customers' rights as legal subjects, as guaranteed by the constitution and laws and regulations.Within the framework of POJK 8/2023, the authorities emphasize consumer protection in the financial services sector through the principles of transparency, accountability, and consent for actions affecting customer rights. Therefore, blocking without consent requires strict legal review from the perspective of banking law, personal data protection, and human rights.

C. Analysis of Principles and Potential Regulatory "Gaps"

According to the analysis, there is a gap between POJK 8/2023, which emphasizes consumer protection and transparency, and the Banking Law, which focuses on confidentiality and trust, particularly when blocking is carried out without adequate consent or notification. The following legal explanation clarifies the point of normative conflict:From a human rights perspective, blocking without consent can be seen as a restriction on the right to ownership and access to private property. Article 28G of the 1945 Constitution guarantees citizens' personal protection and privacy rights. When accounts are blocked without notification and without a clear defense mechanism (Seri Mughni Sulubara et al., 2025), there is a potential violation of due process of law because customers are not given the opportunity to defend themselves before their rights are restricted.The principle of legality and legal certainty requires that any restrictive action have a clear legal basis and measurable procedures. Blocking without approval often relies on broad interpretations of financial institutions' authority, creating legal uncertainty and demonstrating a lack of synchronization between POJK 8/2023 and the Banking Law.The presumption of innocence principle often stems from allegations of involvement in criminal activity (e.g., online gambling or money laundering) (Syarif et al., 2024). However, such actions potentially violate the presumption of innocence principle if taken before a final and binding court decision. The risk of criminalization for customers whose involvement has not been proven is a serious consequence (Kambey & Lengkong, 2025).

Principle of Proportionality and Prudential Principle: In line with POJK 8/2023, banking actions must be proportional and prudent. Blocking must consider the impact on customer rights versus the prevention objective (Dahlan et al., 2025). Without a clear mechanism, blocking policies risk causing losses that outweigh the benefits (Rumondor et al., 2024). Personal Data Protection Regime (PDP Law): Law No. 27 of 2022 defines account data as personal data that must be protected. Blocking data without consent and without a legitimate basis for processing can be considered unauthorized data processing, potentially violating the principles of confidentiality, benefit, and balance in the PDP Law.Harmonization Direction and Implications: Regulatory harmonization is needed between POJK 8/2023, the Banking Law, the Consumer Protection Law, and the Data Protection and Data Protection Law to ensure that law enforcement interests do not override customer rights. If the blocking practice ignores the principles of the Presumption of Innocence and Legal Protection, such action could potentially be classified as abuse of authority by the bank. From a data protection perspective, blocking without consent can also be categorized as unauthorized data processing, thus violating the law under the Data Protection and Data Protection Law. Synchronizing the

above norms is crucial to ensure effective crime prevention while maintaining legal certainty and customer constitutional rights.

Legal Policy Updates Regarding Account Blocking from the Perspective of Banking Law and Future Personal Data Protection

POJK 8/2023 essentially provides a normative basis for banks to block accounts within the framework of preventing money laundering and terrorism financing. However, its implementation in practice still creates legal uncertainty, particularly regarding customers' rights to information and consent to actions that restrict account access (Willyams & Yusuf, n.d.). This situation emphasizes the need for regulatory updates and refinements to ensure that operational standards for blocking align with consumer protection principles and the right to privacy.As a derivative of the 2022 Personal Data Protection Law, the Draft Government Regulation (RPP) on Personal Data Protection is expected to clarify data protection mechanisms, including specific obligations for financial institutions in managing, storing, and processing customer data (Puspita Sari et al., 2024). By establishing strict sanctions for violations, the integration of the Draft Government Regulation on Personal Data Protection (RPP) and POJK 8/2023 has the potential to strengthen customers' position as legal subjects, ensuring transparency in the process and protecting privacy during blocking actions.In terms of principles, POJK 8/2023 does not fully explicitly reflect the principles of data minimization and accountability as adopted by the European Union's General Data Protection Regulation (GDPR).

The GDPR places individual rights at the center of protection through seven key principles: lawfulness, fairness, transparency; purpose limitation; data minimization; accuracy; storage limitation; integrity and confidentiality; and accountability. The framework requires lawful and proportionate processing, and provides for a right to object and due process in data processing. In domestic practice, account blocking is often carried out on suspicion without a clear objection procedure from customers (Kinanti et al., 2025), which differs from GDPR standards, which require remedial action before or during the implementation of restrictive measures.Experience in the European Union shows that compliance with the GDPR is strictly enforced, with data protection authorities in various countries imposing significant sanctions for violations, including substantial fines for technology companies. This practice confirms that personal data protection is viewed as a fundamental human right that requires effective law enforcement, not simply an administrative formality.Going forward, Indonesia can learn from the European model, particularly in strengthening independent supervisory institutions to ensure bank compliance with the PDP Law and the POJK. Proportionate yet sufficiently severe administrative and criminal sanctions should be imposed for violations of customer data processing. Similarly, accessible complaint and mediation mechanisms should be developed for customers whose accounts are blocked without transparent procedures, so that a balance between law enforcement and the protection of customer rights can be effectively achieved.

IV. CONCLUSION

First. Within the framework of the Personal Data Protection Law (PDP Law), account data is classified as personal data subject to confidentiality and lawful processing obligations. Therefore, blocking an account without consent can be viewed as data processing that lacks a sufficient legal basis, potentially violating the principle of personal data protection. On the other hand, the Banking Law allows for restrictions on account access in the context of law enforcement—for example, at the request of authorized officials (police, prosecutors, judges, the Corruption Eradication Commission), to prevent money laundering, and to protect the stability of the financial system. Meanwhile, POJK 8/2023 emphasizes that actions impacting customer rights must be carried out transparently and with the account holder's knowledge. The combination of these three regulatory regimes indicates a normative disharmony, particularly when blocking is carried out without consent/notification.

Therefore, harmonization between POJK 8/2023, the PDP Law, and the Banking Law is imperative, while upholding the principles of equality before the law and the presumption of innocence, so that law enforcement interests do not override customer rights as protected legal subjects.Second, Indonesia needs to strengthen its due process, establish a clear and accessible objection mechanism, and enforce strict sanctions

against violations of customer personal data protection. Lessons learned from the European Union's GDPR framework, which prioritizes the principles of lawfulness, fairness, transparency; purpose limitation; data minimization; accuracy; storage limitation; integrity and confidentiality; and accountability, can be used as a reference for placing individual rights at the center of legal protection in account blocking practices. Going forward, gaps/weaknesses in the objection procedure need to be addressed through more detailed regulations, so that national standards increasingly align with international practices in protecting customer rights in the financial services sector.

V. SUGGESTION

Regulators (OJK and the Government) need to develop detailed derivative regulations regarding account blocking procedures, including mandatory notification requirements for customers, procedures for filing objections or mediation, and transparency standards that banks must meet. Normative integration between POJK No. 8 of 2023 and the Personal Data Protection Law through government regulations will strengthen legal certainty and protect customer rights. In this context, policymakers (legislators and executives) need to prioritize cross-regulatory harmonization, particularly between the PDP Law, the Banking Law, the Consumer Protection Law, and POJK 8/2023, to create a balance between law enforcement and the protection of human rights, including the right to privacy and access to assets.

On the other hand, banks need to establish standard operating procedures that prioritize the principles of prudence and proportionality, by ensuring that every blocking action is based on a clear legal basis, accompanied by official notification, and the availability of communication channels for clarification and remediation. Strengthening governance, decision documentation, and audit trails are crucial to ensure the accountability of bank actions. In parallel, customers need to be encouraged through increased legal and financial literacy to understand their rights to personal data protection and account blocking mechanisms, so they can proactively use objection and dispute resolution tools in the event of an unprocedural blocking. Furthermore, academics and legal practitioners are expected to expand comparative studies with international regulations, such as the GDPR, and conduct further research on the effectiveness of objection mechanisms, civil and criminal implications, and independent oversight models as a basis for strengthening customer protection policies and practices.

REFERENCES

[1] Angelica Putri Siagian, Z., & Dompak, T. (nd). The important role of human rights protection in the constitutional law system. https://ijurnal.com/1/index.php/jrpu

[2] Angraini K, N., Makkawaru, Z., & Almusawir, A. (2024). Legal protection of personal data from a human rights perspective. ***Indonesian Journal of Legality of Law***, 7(1), 46–51. https://doi.org/10.35965/ijlf.v7i1.5267

[3] Apriandi, M., Valentina Sagala, R., & Artikel, R. (nd). Legal protection for cybercrime victims of online dissemination of personal data. INFO ARTIKEL, 1(11), 1069–1079. https://doi.org/10.62335

[4] Aprilia, VM, Doodoh, MA, & Lambonan, ML (2025). A legal review of personal data protection in addressing cybercrime in phishing cases. ***Unsrat Faculty of Law Journal***, 14.

[5] Dahlan, S., Hasan, YA, & Almusawir, A. (2025). Implementation of customer personal data protection through banking institutions in Makassar. ***Indonesian Journal of Legality of Law***, 7(2), 217–224. https://doi.org/10.35965/ijlf.v7i2.6075

[6] Doodoh, M., & Tuwaidan, HFD (2025). A human rights perspective on the presumption of innocence in Indonesian criminal law. ***Jurnal Nuansa Akademik: Jurnal Pembangunan Masyarakat***, 10(1), 95–106.

[7] Gunardi, SH, MH (2022). Legal research methods.

[8] Muhaimin, SH, MH (2020). Legal research methods.

[9] Kambey, TJ, & Lengkong, MR (2025). Application of the principle of presumption of innocence in the Indonesian criminal justice system: Analysis of court decisions 2020–2024. ***MKJ Journal***, 2(1). https://naluriedukasi.com/index.php/mahkamahhukumjournal/index

[10] Karso, AJ (2025). Blocking of dormant accounts by PPATK as an anticipatory measure to break the chain of online gambling in Indonesia. Publisher: CV Eureka Media Aksara.

[11] Kinanti, W., Ramadhani, S., & Wiraguna, SA (2025). Implementation of personal data protection in information systems at financial services companies. Public Administration and Law Perspectives, 2(2), 158–175. https://doi.org/10.62383/perspektif.v2i2.248

[12] Maria Aritonang, L., & Handayani, R. (2025). Legal analysis of personal data leaks and identity misuse in banking based on Law Number 27 of 2022 concerning Personal Data Protection. R2J, 7(5), 3146. https://doi.org/10.38035/rrj.v7i5

[13] Niken, R., & Diena, M. (2024). Implications of changes in AML regulations and personal data protection on banking profitability. ***Student Research Scientific Journal***, 2, 1–11.

[14] Puspita Sari, H., Nilamsari, MA, Sitorus, DF, Harimurti, YW, Telang, JR, Kamal, K., Bangkalan, K., Timur, J., & Penulis, K. (2024). Effectiveness of personal data protection law against cybercrime in Indonesia. ***JMA,*** 2(11), 3031–5220. https://doi.org/10.62281

[15] Rumondor, S., Kapugu, BA, & Wahongan, AS (2024). Personal data protection in the face of cybercrime through digital banking transactions. Lex Privatum, 13(5).

[16] Sembiring, S., & Hum, M. (2024). Banking and financing institution law. Publisher: CV Eureka Media Aksara.

[17] Sulubara, SM, Fauzi, H., Muslim, B., Putra, MFF, & Musmulyadi. (2025). Online gambling as cybercrime and the challenges of criminal law enforcement in the digital era. ***Journal of Research in the Social, Political and Humanities Sciences Cluster***, 4(2), 539–552. https://doi.org/10.55606/jurrish.v4i2.4990

[18] Sholat, J., & Apriandani, B. (2024). Legal protection for victims of technological crimes in Indonesia. ***Journal of Non-Discriminatory Law (JHND)***, 3(1), 158–162. https://doi.org/10.56854/jhdn.v3i1.449

[19] Sidi, I., Wiraguna, A., Ars, M., & Barthos, M. (2025). Privacy law and personal data protection in Indonesia (SH Neng Rismawati, Ed.; 1st ed.). Widina Media Utama.

[20] Syarif, N., Januri, J., & Saribu, ELD (2024). Protection of suspects' rights through the presumption of innocence in the criminal justice system. Audi et AP: ***Journal of Legal Research***, 3(2), 112–120. https://doi.org/10.24967/jaeap.v3i02.3310

[21] Willyams, FJ, & Yusuf, H. (nd). The role of the Financial Services Authority in preventing banking crimes and money laundering in Indonesia. ***JIIC: Jurnal Intelek Insan Cendikia***. https://jicnusantara.com/index.php/jiic