JCRD: Journal of Citizen Research and Development
E-ISSN: 3048-2941 P-ISSN: 3048-2933
Vol. 3 No. 1 May 2026

Legal Protection for Banking Customers Regarding Personal Data Information in the Perspective of Legal Certainty

M Ridho[1] Taufik Yahya[2] Indriya Fathni[3]
Master of Law Study Program, Faculty of Law, Jambi University, Jambi Indonesia[1,2,3]
Email: ridhom437@gmail.com[1] taufik_yahya@unja.ac.id[2] indriya.fathni@gmail.com[3]

Abstract
The development of information technology and the digitalization of banking services has increased the utilization of customers' personal data in various financial transactions. On the other hand, this situation also poses risks of misuse of access and leakage of personal data. Therefore, clear legal regulation that provides legal certainty is crucial to ensure the protection of personal data in the banking sector. This study aims to analyze the legal regulation of personal data protection in the banking sector from the perspective of legal certainty and to examine the forms of legal protection provided to customers regarding access to personal data information in Indonesia. This research employs a normative legal research method with a statute approach and a conceptual approach. The legal materials used include legislation, specifically Law Number 10 of 1998 concerning Banking, Law Number 27 of 2022 concerning Personal Data Protection, as well as various financial sector regulations issued by the Financial Services Authority and Bank Indonesia. The analysis is conducted using the theory of legal certainty and the principle of conflict resolution of norms, namely lex specialis derogat legi generali and lex posterior derogat legi priori. The results of the study indicate that the regulation of personal data protection in the banking sector essentially has a sufficient legal foundation through provisions on bank secrecy in the Banking Law and general personal data protection regulations in the Personal Data Protection Law. However, there is a potential overlap of norms between these two legal regimes, particularly regarding state access to data and the obligations of data controllers. Furthermore, the fragmentation of supervisory authority among the Financial Services Authority, Bank Indonesia, and law enforcement agencies may lead to inconsistencies in the procedures for access and protection of customer data. Legal protection for customers can be provided through preventive mechanisms, such as banks' obligations to maintain data confidentiality and implement electronic system security, as well as repressive mechanisms through complaints, dispute resolution, administrative sanctions, and criminal sanctions based on the applicable legislation. Based on indicators of legal certainty, the existing regulations have provided a normative basis for the protection of customers' personal data, but regulatory harmonization and strengthening of supervisory mechanisms are still required to ensure effective legal protection of personal data in the digital banking era.
Keywords: Personal Data Protection, Bank Secrecy, Legal Certainty, Customer, Banking Sector

INTRODUCTION

Law is a unique field of knowledge (sui generis) because its object of study differs from other disciplines, namely the norms and rules that govern social life.[1] Through scientific research, law is developed to understand legal objectives, the value of justice, and the validity of norms applicable within society. Beyond being a system of norms, law also functions as a practical guide for regulating various social and economic activities. In the context of modern economic activities, one legal branch that plays a vital role is business law, which regulates legal relationships in economic activities carried out by individuals, business entities, and financial institutions.[2] One sector with a strategic role in the economic system is the banking sector. Banking serves a primary function as an intermediary institution that collects funds from the public and redistributes them in the form of credit or other financial services.[3] This function is emphasized in Law Number 10 of 1998 concerning Banking, which states that banking plays

a role in supporting national development to improve equity, economic growth, and national stability. In performing this function, banks also act as an agent of trust, making public trust a crucial element in banking operations. One form of protection for customer interests in banking activities is the implementation of the principle of bank secrecy. This principle requires banks to maintain the confidentiality of information regarding depositing customers and their deposits, as regulated in Article 40 of Law Number 10 of 1998 concerning Banking. These provisions aim to protect customer interests and maintain public trust in banking institutions. However, the principle of bank secrecy in the Indonesian legal system is not absolute because laws and regulations provide certain exceptions, such as for taxation purposes, state debt settlement, or judicial processes, as regulated in Articles 41 to 44A of the aforementioned law.

The development of information technology and the digitalization of financial services have changed how banks manage customer information. Data managed by banks is no longer limited to deposit information but also includes identity data, electronic transaction data, and various other forms of digital data that can identify an individual. This condition demands more comprehensive legal protection for customer personal data. Consequently, the state enacted Law Number 27 of 2022 concerning Personal Data Protection, which provides a legal framework for personal data protection as part of individual privacy rights guaranteed under the 1945 Constitution of the Republic of Indonesia, specifically Article 28G paragraph (1), which guarantees protection for the person, honor, and sense of security of every individual. In practice, the development of digital banking services also increases the risk of leaks or misuse of customer personal data. Cases of leakage and misuse of customer personal data have occurred, such as the matter examined in Court Decision Number 230/Pdt.G/2022/PN Kpg at the Kupang District Court. This case began when a customer experienced unauthorized transactions on a mobile banking service, resulting in a significant reduction in account balance. Such cases demonstrate that the management and protection of customer data in digital banking systems still face various challenges, especially in ensuring secure data access and preventing misuse by unauthorized parties. This situation raises questions regarding the extent of a bank's responsibility in protecting customer personal data and the legal protection mechanisms available to customers when a breach of their personal data security occurs.

On the other hand, the state also has an interest in accessing public financial information to support law enforcement and optimize state revenue. This is regulated through Law Number 9 of 2017 concerning Access to Financial Information for Taxation Purposes, which grants tax authorities the power to obtain financial information from financial service institutions. These regulations indicate a need to balance the protection of confidentiality and customer personal data with the state's interest in conducting supervision and law enforcement in the financial sector. Based on these conditions, this research focuses its study on the legal regulations governing the protection of customer personal data in the banking sector and the legal protection mechanisms that can be provided to customers regarding access to their personal data within the Indonesian legal system. Thus, this study examines the form of legal regulation of personal data protection in banking when viewed from the principle of legal certainty, as well as the form of legal protection for banking customers regarding personal data access in Indonesia. This research also aims to identify and analyze the legal regulations governing personal data protection in the banking sector and to explain the forms of legal protection that can be provided to customers over access to their personal data in the practice of providing banking services.

General Overview of Banking

1. Definition and Legal Basis of Banking. Etymologically, the term bank originates from the Italian word banco, which means a bench or table used for money exchange activities during

the early development of banking in Europe. Juridically, the definition of a bank in Indonesia is regulated under Law Number 10 of 1998 concerning Banking as an amendment to Law Number 7 of 1992 concerning Banking. Article 1, paragraph (2) states that a bank is a business entity that collects funds from the public in the form of deposits and redistributes them in the form of credit or other forms to improve the standard of living of the masses. Thus, a bank is a financial institution that performs an intermediary function and operates within the framework of the legal system governing banking activities.

2. Function and Purpose of Banking. A bank functions as a financial intermediary institution (financial intermediary) that collects funds from the public in the form of deposits and redistributes them as credit or financing to support economic activities. Additionally, banks also serve as an agent of trust, agent of development, and agent of services, reflecting their role in building public trust, driving economic development, and providing various financial services. In line with these functions, the purpose of banking, as regulated in Law Number 10 of 1998, is to support the implementation of national development to increase economic growth and public welfare.
3. Types and Banking Systems in Indonesia. Based on Law Number 10 of 1998, the types of banks in Indonesia consist of Commercial Banks (Bank Umum) and Rural Banks (Bank Perkreditan Rakyat - BPR), which differ in their scope of business activities. Furthermore, Indonesia recognizes Sharia banking, which is regulated under Law Number 21 of 2008 concerning Sharia Banking. The Indonesian banking system adheres to a dual banking system, where conventional and Sharia banking operate side-by-side under the supervision of the Financial Services Authority (Otoritas Jasa Keuangan - OJK), while monetary policy and the payment system remain the authority of Bank Indonesia.
4. Legal Relationship Between Banks and Customers. A customer is a party that has a legal relationship with a bank as a depositor of funds or a user of banking services; thus, this creates a civil relationship based on an agreement and is subject to the principles of freedom of contract and good faith. In this relationship, the bank is responsible for maintaining the security and confidentiality of customer data according to the provisions of Law Number 10 of 1998 and can be held liable if an error or negligence occurs that results in losses, based on Article 1365 of the Civil Code.
5. Principles of Banking Law. The principles of banking law include the principle of prudence (prudential principle), the principle of bank secrecy, and the "Know Your Customer" (KYC) principle. The principle of prudence requires banks to conduct their business in a careful and responsible manner as regulated in Article 2 and Article 29 of Law Number 10 of 1998. The principle of bank secrecy obligates banks to maintain the confidentiality of customer data according to Article 40 of said law, while the KYC principle requires banks to identify and monitor customers as regulated in Bank Indonesia Regulation Number 3/10/PBI/2001.
6. Bank Secrecy and its Relevance to Data Protection. In banking law, there are theories of absolute and relative bank secrecy; the Indonesian legal system adopts the relative theory, which allows the opening of bank secrets under certain conditions as regulated in Law Number 10 of 1998. Along with technological developments, protection also extends to personal customer data as regulated in Law Number 27 of 2022 concerning Personal Data Protection, necessitating the harmonization of these two regulations.
7. Consumer Protection in the Banking Sector. Consumer protection in the banking sector aims to guarantee legal certainty and balance in the relationship between banks and customers. Its regulation is under the Financial Services Authority (OJK) based on Law Number 21 of 2011, and it is also supported by Law Number 8 of 1999 concerning Consumer Protection, which guarantees consumer rights to information, security, and dispute resolution.

Legal Regulation of Personal Data Information Access

1. The Concept of Personal Data Access in a Legal Perspective. Access to personal data encompasses every form of processing that must be based on a valid legal basis and a clear purpose, as regulated under Law Number 27 of 2022 concerning Personal Data Protection. In practice, such access must adhere to data protection principles such as legality, purpose limitation, and security to guarantee privacy protection and legal certainty, particularly within the banking sector.
2. Regulation of Personal Data Access under Law Number 27 of 2022. On Personal Data Protection Under Law Number 27 of 2022 concerning Personal Data Protection, data subjects possess the right to access and control their personal data, while data controllers are obligated to ensure security and are held responsible for any violations. However, its implementation still faces challenges, especially regarding technical standards and the evidentiary process for data breaches.
3. Regulation of Customer Data Access in Banking Law. Access to customer data is restricted by the principle of bank secrecy as stipulated in Law Number 10 of 1998 concerning Banking; however, it may be disclosed on a limited basis for specific legal interests through strict procedures and the supervision of the Financial Services Authority (OJK).
4. Data Access by the State and Law Enforcement Agencies. Data access by the state is restricted by the principles of legality and proportionality and may only be conducted for specific legal interests in accordance with Law Number 10 of 1998 concerning Banking and Law Number 27 of 2022 concerning Personal Data Protection, in order to maintain a balance between state interests and customer privacy.
5. Data Access by Third Parties and Technology Partners. The development of digital banking has encouraged collaboration between banks and third parties, such as fintech companies and technology providers, which expands the processing of customer data and increases the risk of breaches. Therefore, clear regulations are required regarding responsibilities, customer consent, and compensation mechanisms, while reaffirming that the bank, as the data controller, is responsible for ensuring data protection in accordance with Law Number 27 of 2022 concerning Personal Data Protection.

Legal Protection for Customers Regarding Personal Data Information Access

Legal Regulation of Customer Personal Data Access in the Indonesian Legal System

The regulation of access and protection of customer personal data within the Indonesian legal system is anchored in Law Number 27 of 2022 concerning Personal Data Protection, which asserts that data processing must be conducted lawfully, transparently, and accountably, based on the principles of legality, purpose limitation, security, and respect for the rights of the data subject. This law also grants individuals the right to access, rectify, restrict, and even demand accountability for the processing of their personal data, while obligating data controllers to guarantee the security and validity of every data processing activity. In the banking context, these provisions serve as a normative basis ensuring that every instance of access to customer data must have a clear legal ground, whether based on consent or legal obligation. In banking law, customer data protection is reinforced through Law Number 10 of 1998 concerning Banking, which regulates the principle of bank secrecy as an obligation to protect customer information, although it is relative in nature as it allows for limited data disclosure for specific interests such as taxation, the judiciary, and the settlement of state receivables. This arrangement demonstrates a balance between the protection of customer privacy and broader legal interests, ensuring that access to data can only be carried out through valid and measurable procedures to guarantee legal certainty and prevent abuse. Furthermore, customer

data protection within the financial services sector is also regulated by Financial Services Authority Regulation (Peraturan Otoritas Jasa Keuangan) Number 22 of 2023, which emphasizes the principles of transparency, fairness, and consumer data security, including in digital services involving third parties. This regulation requires financial service providers to maintain data confidentiality, provide complaint mechanisms, and submit to the supervision of the Financial Services Authority, thereby forming a comprehensive legal protection framework and ensuring that the management of customer data is conducted responsibly within the modern financial ecosystem.

Forms of Legal Protection for Customers Against Personal Data Access

Legal protection for the access to customer personal data information in the banking sector is divided into two primary forms: preventive and repressive legal protection. Preventive protection functions to prevent violations through regulation, supervision, and the implementation of the prudential principle in data management, while repressive protection aims to provide recovery and law enforcement if a violation has occurred. These two forms complement each other in guaranteeing customer privacy rights and creating legal certainty amidst the development of digital banking services. Preventive legal protection is realized through various regulations governing a bank's obligation to maintain the confidentiality and security of customer data, such as bank secrecy provisions, electronic system security, and personal data protection. The obligation to keep customer data confidential serves as the primary basis for preventing unauthorized access, with limited exceptions strictly regulated by law. Furthermore, banks are required to implement information technology security systems, including access restrictions, data encryption, and internal supervision to minimize the risk of data breaches.

In the digital era, preventive protection is further strengthened through the application of personal data protection principles, such as legality, purpose limitation, data minimization, accountability, and security. These principles require every instance of data processing to have a clear legal basis, be conducted transparently, and remain accountable. Additionally, customer consent and information transparency become vital instruments in providing customers with control over the use of their personal data. Meanwhile, repressive legal protection provides resolution mechanisms if a data access violation occurs. Customers may file complaints with the bank, pursue dispute resolution through alternative institutions, and obtain protection through the supervision of the financial services authority. Moreover, personal data violations can be subject to administrative or criminal sanctions, against both individuals and corporations, as a form of law enforcement and to provide a deterrent effect. Overall, the legal protection system for customer personal data in Indonesia encompasses comprehensive prevention and enforcement efforts. Its effectiveness relies heavily on the consistency of law enforcement, optimal supervision, and the readiness of banking institutions to implement data security standards. Thus, the combination of preventive and repressive protection is key to maintaining public trust and ensuring the protection of customer privacy rights in the modern banking system.

Legal Certainty Analysis of Customer Personal Data Access

The analysis of legal certainty regarding access to customers' personal data information reveals potential conflicts of norms due to the existence of several regulations with different scopes, specifically between the Banking Law and the Personal Data Protection Law. The Banking Law focuses on the principle of confidentiality of customers' financial information, whereas the Personal Data Protection Law provides broader protection for all data that can

identify an individual. This difference in orientation has the potential to cause overlapping norms, particularly in the context of digital banking which involves complex data processing, thereby creating a need for aligned and integrated legal interpretation. Potential conflicts are also evident in the mechanisms for data access by the state and the obligations of data controllers. On one hand, the Banking Law allows for the disclosure of bank secrets under certain conditions for legal and state interests; on the other hand, the Personal Data Protection Law demands a valid legal basis, purpose limitation, and protection of the data subject's rights. This difference creates a normative dilemma for banks in determining which compliance standards should be prioritized. Therefore, the application of the lex specialis and lex posterior principles must be carried out carefully while still considering the objectives of privacy rights protection and legal certainty.

In addition to the conflict of norms, there is also a fragmentation of supervisory authority involving various institutions such as the Financial Services Authority (OJK), Bank Indonesia, law enforcement agencies, and tax authorities. Each institution has different legal bases and interests in accessing customer data, which potentially leads to unsynchronized procedures and operational standards. This condition not only makes it difficult for banks to ensure compliance with all regulations but also creates ambiguity for customers regarding which parties are authorized to access their data and the limits of its use. From the perspective of legal certainty, these conditions demand regulatory harmonization and strengthened coordination between institutions. Joint guidelines are needed to regulate data access procedures, usage limits, as well as integrated supervision and accountability mechanisms. In this way, the protection of customers' personal data can be balanced between the interests of supervision and law enforcement and the guarantee of individual privacy rights, thereby increasing public trust in the banking system in the digital era.

CONCLUSION

Based on the discussion in this research, it can be concluded that: The legal regulation of customer personal data protection in the Indonesian banking sector has a sufficient normative basis through various laws and regulations. These provisions are reflected in the Banking Law, which emphasizes the principle of bank secrecy, and in the Personal Data Protection Law, which comprehensively regulates data processing and the rights of data subjects. Nevertheless, from the perspective of legal certainty, issues remain in the form of potential overlapping norms between regulations, fragmentation of supervisory authority, and suboptimal technical regulations—particularly in the context of digital banking. Therefore, regulatory harmonization is required to strengthen legal certainty. The forms of legal protection for customers regarding personal data access are divided into preventive and repressive protection. Preventive protection is realized through the obligation to maintain data confidentiality, the implementation of electronic system security, data subject consent, transparency of information, and supervision by relevant authorities. Meanwhile, repressive protection is carried out through complaint mechanisms, dispute resolution, administrative sanctions, and criminal law enforcement. However, the effectiveness of such protection still faces challenges, such as the complexity of evidence in digital systems, the involvement of third parties, and suboptimal coordination between institutions. Consequently, it is necessary to strengthen regulatory harmonization, improve data security standards, and optimize supervision and law enforcement to ensure more effective protection of customer personal data.

Recommendations

Based on the research conclusions, the following suggestions are proposed: Harmonization and synchronization of regulations between the Banking Law and the Personal Data Protection Law are required to prevent normative conflicts in the regulation of confidentiality and customer data access. The government and lawmakers need to clarify the relationship between these two legal regimes, including the limits of data access authority by the state and data disclosure procedures that continue to guarantee the protection of customer privacy rights. The Financial Services Authority (OJK) needs to strengthen technical regulations in the banking sector, particularly regarding electronic system security standards, customer data governance, and data breach risk management, especially in collaborations with third parties. This reinforcement is essential so that banks can effectively implement modern data protection principles—such as legality, purpose limitation, data minimization, accountability, and security—within their operations. Banking institutions need to improve data protection governance through the implementation of comprehensive information security systems and transparency toward customers regarding the processing of personal data. Banks must also ensure that every collaboration with third parties is equipped with clear arrangements regarding responsibility, supervision, and data breach handling, in order to prevent misuse and strengthen public trust in the banking system.

BIBLIOGRAPHY

(1) Muhaimin. 2020. Metode Penelitian Hukum. Mataram: Mataram University Press.
(2) Sobirin Malian. 2017. Pengantar Hukum Bisnis. Yogyakarta: Kreasi Total Media.
(3) Karmila Sari Sukarno. 2025. Fungsi Bank Sebagai Agen Pembangunan (Agent of Development) Menuju Indonesia Emas 2045. Jurnal Madani Hukum. Vol. 3. No. 1.
(4) Chika Ghassani, Fadhil Pratama Putra, dan Zainudin Firdaus. 2025. Analisis Yuridis Terhadap Tanggung Jawab Perdata Atas Kebocoran Data Pribadi Nasabah Oleh PT. Bank Central Asia Cabang Kupang (Studi Putusan Pengadilan Negeri Kupang Nomor 230/PDT.G/2022/PN KPG, Juris Prudentia: Jurnal Hukum Ekselen. Vol. 7. No. 2.
(5) Agus Bandiyono dan Ayudya Purwani Putri. 2021. Analisis Keterbukaan Akses Informasi Keuangan Dalam Peningkatan Penerimaan Pajak. Jurnal Ilmiah Akuntansi Universitas Pamulang. Vol. 9. No. 2.
(6) Dhoni Martien.2023. Perlindungan Hukum Data Pribadi, Makassar: Mitra Ilmu.
(7) Nayla Azarine, Tesalonika David, dan Valsifa Utami. 2024. Upaya Perlindungan Hukum terhadap Nasabah Perbankan melalui Prinsip Kerahasiaan Bank dalam UU No. 4 Tahun 2023 tentang Pengembangan dan Penguatan Sektor Keuangan. Jurnal Pajak dan Manajemen Keuangan. Vol. 1 No. 5.