American Journal of Humanities and Social Sciences Research (AJHSSR)
e-ISSN : 2378-703X
Volume-09, Issue-08, pp-07-13
www.ajhssr.com
Research Paper Open Access

BANK'S ROLE IN SAFEGUARDING THE CONFIDENTIALITY OF THEIR CUSTOMERS' PERSONAL DATA

Michael Santosa[1], Endang Retnowati[2], Fries Melia Salviana[3]
[1,2,3]*Fakultas Hukum, Universitas Wijaya Kusuma Surabaya, Indonesia.*

ABSTRACT : The rapid rise in threats to customers' personal data—driven by the exponential growth of digital information technology—has created an urgent need for comprehensive legal safeguards within the banking sector. In Indonesia, these protections are enshrined in Law No. 4 of 2023 on the Development and Strengthening of the Financial Sector, Law No. 27 of 2022 on Personal Data Protection, and Financial Services Authority Regulation No. 44 of 2024 concerning Banking Secrecy. This thesis seeks to analyze the nature and scope of banks' legal liabilities under the applicable statutes and to evaluate the relevance of the Personal Data Protection Law and FSA Regulation No. 44/2024 as instruments for reinforcing those safeguards. Employing a normative-juridical approach, the study relies on statutory analysis and documentary review. Findings indicate that banks are duty-bound to protect customers' personal data through rigorous security systems and bear full responsibility for any data breaches. This duty encompasses legal, technical, and ethical obligations inherent in the bank's role as a data controller. Consequently, strengthening protective mechanisms through collaboration among banks, regulators, and the public is imperative. The key recommendations are adopting adaptive security technologies, enhancing human-resource capacity, conducting periodic data-security audits and educating customers about their personal-data rights.

Keywords: *Customers' Personal Data, Legal Responsibility, Banking.*

I. INTRODUCTION

Advancements in information technology have revolutionized the way banks store and manage customers' personal data. In just the last decade, banks have ceased to be mere financial intermediaries and have become custodians of highly valuable personal information. Accordingly, they bear both moral and legal obligations to guarantee the security and confidentiality of that data.

Rapid technological progress has given rise to a variety of new banking services, precipitating a shift from conventional to digital systems and transforming transaction methods—most notably through the advent of internet banking.

Internet banking is offered to simplify customers' transactions; yet, like two sides of the same coin, these innovations bring both tremendous convenience and novel risks. A classic concern among customers is security: they demand not only ease of use but also assurance that their assets will not be diminished and their personal data not misused.

As the data controller, a bank is obliged to ensure that its services are both secure and non-detrimental to customers. This duty is established in several key statutes: Law No. 27 of 2022 on Personal Data Protection (hereinafter, the "Personal Data Protection Law"); Law No. 7 of 1992 on Banking (the "1992 Banking Law"), as amended by Law No. 10 of 1998 (the "1998 Banking Law"); and Law No. 4 of 2023 on the Development and Strengthening of the Financial Sector (the "P2SK Law"). Under these laws, banks must adopt cutting-edge security measures—such as data encryption, firewall systems, and two-factor authentication— to guard customer information against unauthorized access. Equally important is cultivating an organizational culture of data protection through regular ethics and security training for employees.

In this era, personal data—ranging from full name and identity number to address and transaction history—has become a high-value asset within the banking sector. If not properly safeguarded under the law, such data can be ripe for misuse. Thus, banks have both technical and juridical duties to protect customers' personal data, grounded in the basic theory of legal protection, which seeks to shield citizens' rights from infringement by any entity handling sensitive information.

Indonesia's comprehensive data-protection regime is a recent development. Prior to 2022, personal data safeguards appeared only in sectoral regulations—most notably Law No. 11 of 2008 on *Informasi dan Transaksi Elektronik* (the "*Undang-undang ITE Tahun 2008*"), as amended by Law No. 19 of 2016 (the "*Undang-undang ITE Tahun 2016*"), and Government Regulation No. 71 of 2019 on Electronic Systems and Transactions. However, the rise of a global digital civilization has made it imperative to enact a unified,

principle-based framework for personal data protection. Social-contract theory, as articulated by philosophers like John Locke, holds that citizens' obligation to obey civil government depends on the state's protection of their inalienable rights—including property rights. In Indonesia, the state's concrete expression of that protection is the Personal Data Protection Law, which provides the primary legal foundation for data privacy.

Under this law, any information that can directly or indirectly identify an individual— what the statute terms "identifiable data"—is classified as personal data requiring protection. The law enshrines privacy as a fundamental right, guarantees data-subject rights (such as access, correction, erasure, and withdrawal of consent), and imposes administrative and criminal sanctions for violations. These provisions reflect the EU's General Data Protection Regulation (GDPR) principles while tailoring them to Indonesia's context. The Personal Data Protection Law thus ensures that banks handle personal data ethically and responsibly.

Specifically for banks, the law regulates data-use principles, data-subject rights, and the obligations of both data controllers and processors, complete with sanctions for noncompliance. Since its enactment, banks are expected to exercise greater care and transparency in leveraging customers' personal data for operational and business purposes. In banking practice, personal data is typically grouped into: Basic personal data (e.g., name, ID number), Financial data (e.g., account balances, transaction history), Behavioral data (e.g., spending patterns, channel usage). Before the Personal Data Protection Law, banks' duty to maintain customer confidentiality was set forth in the 1998 Banking Law; the P2SK Law later clarified and reinforced that duty. Known as "banking secrecy," this obligation can be waived only with the customer's consent or under narrowly defined legal exceptions. Consequently, studying the harmonization of these overlapping statutes is critical to addressing contemporary issues in
personal data protection.

Therefore, based on the issues and urgency outlined above, in order to dive to a deeper understanding of the harmonization and effectiveness of the statutory framework governing the protection of bank customers' personal data, the author examines and analyzes the role of banks in safeguarding and ensuring the condifentiality of their customers' personal information.

II. RESEARCH METHOD

In this study, a normative legal research method is employed, supported by a single analytical instrument: the Statute Approach (Pendekatan Peraturan Perundang-undangan). The Statute Approach is utilized because the relevant legal provisions constitute the focal point of this research..

III. RESULTS AND ANALYSIS

3.1 The Relationship between the Bank and It's Customers.

In today's information-technology era, consumer trust is the foremost tool businesses use to attract as many customers as possible. In the banking industry, one of the primary "capitals" for acquiring new clients is convincing them that the confidentiality of their personal data is a fundamental priority in securing public confidence in banking institutions.

The bank–customer relationship is principally grounded in civil-law doctrines, banking law, and consumer-protection law. This legal framework gives rise to both rights and obligations on the part of the bank to safeguard customers' interests—whether related to deposits, loans, or other financial services—all of which form an integral part of the modern financial system.

At its core, the bank–customer relationship is a civil-law relationship based on contract. It originates from the mutual agreement of both parties, typically embodied in a written contract. Article 1313 of the Indonesian Civil Code provides that: "An agreement is an act by which one person or more bind themselves to one person or more other persons." This contractual foundation underpins the legal obligations of banks to protect the confidentiality and integrity of customer data.

In this context, when a customer opens an account, takes out a loan, or uses any other service, the moment they sign the account-opening form—which contains clauses setting forth rights and obligations—a legally binding contract is formed between that customer and the bank. In the banking system, the customer occupies a foundational role in the bank's operations: customers are the vital asset that enables the bank to conduct its business. Broadly speaking, customers fall into two categories: depositors and borrowers. Although their positions and interests differ, both are interdependent within the banking system. A clear understanding of these two customer types is crucial not only for financial institutions but also for the public as participants in economic transactions.

A depositor is a party that places its own funds with the bank in the form of deposits. Pursuant to Article 14(1)(5) of Law No. 4 of 2023 on the Development and Strengthening of the Financial Sector (the P2SK Law), a 'deposit' is defined as: "Funds entrusted by the public to the bank in the form of demand deposits, time deposits, certificates of deposit, savings, and/or other forms deemed equivalent thereto".

Furthermore, as stipulated in Article 14(1)(17) of Law No. 4 of 2023 on the Development and

Strengthening of the Financial Sector (P2SK Law), a 'depositor' is defined as a party that places its funds in the bank in the form of deposits under an agreement between the bank and the relevant customer. Accordingly, a depositor may be understood as an individual or legal entity that entrusts its money to the bank in the form of savings accounts, demand deposits, time deposits, or other equivalent banking products. Depositors place their funds in banks for several purposes: security, earning interest, and transactional convenience. By depositing their funds, depositors receive returns according to the product type—such as interest on demand and time deposits or profit-sharing in Islamic banking. The bank is then obligated to safeguard and guarantee the security of all funds entrusted by its depositors. In contrast to depositors, the second category of customers is borrowers—those who obtain funds from the bank in the form of credit or financing. Although the term 'borrower' is not explicitly detailed in the 1998 Banking Law, it corresponds to the concept of a debtor in banking practice.

A borrowing customer is a business entity or individual who receives credit from the bank for purposes of consumption, investment, or working capital, which must be repaid within an agreed term and at an agreed interest rate or margin as specified in the contract. Borrowers are obligated to repay their loans in accordance with the agreement, including any agreed interest or margin. Loan facilities extended to borrowers become a primary source of income for the bank and underscore the bank's core function as a financial intermediary.

The principal distinction between these two customer types lies in the direction of funds: depositors place funds with the bank, whereas borrowers draw funds from the bank. Each plays a vital role in maintaining the balance of the banking system. Funds mobilized from depositors are, in turn, channeled as credit to borrowing customers

Depositors and borrowers are two pivotal entities in the banking mechanism. Both occupy legal positions governed by statute and possess distinct rights and obligations. Understanding the differences and roles of each customer type is crucial to fostering a fair, transparent, and accountable relationship between the bank and its clients. With appropriate legal protection, both depositors and borrowers can perform their roles optimally within the national financial system. In Indonesia, regulations on personal-data protection are not intended to hinder corporate activity; we all recognize that data today constitutes a strategic and competitive asset for modern corporations—not only in banking but across all industries—and is essential for maintaining an edge in international competition. Moreover, personal data is now required to optimize the delivery of best-in-class services to customers and anyone interacting with a modern corporate business system.

The Personal Data Protection Law was enacted as an adaptation to the evolution of global corporations. Its drafting was guided by the European Union's General Data Protection Regulation (GDPR) and international best practices. Therefore, certification standards aligned with the GDPR can serve as useful benchmarks. Such standards play a critical role in evidentiary processes within the judicial system, influencing court rulings on criminal liability. Standards and law are thus deeply interrelated, especially when demonstrating corporate compliance in court. As a financial institution entrusted with public confidence, a bank handles various categories of customers' personal data—including identity details, financial transactions, location information, and other sensitive data. Accordingly, safeguarding banking secrecy cannot be divorced from protecting customers' personal data. Under Indonesian law, these two concepts—personal data and banking secrecy—each rest on a solid legal foundation, even though they arise from different legal regimes. Their relationship is so closely intertwined that a breach of one almost invariably entails a breach of the other.

The P2SK Law explicitly governs banking secrecy and depositor data, which legally encompasses customers' personal information that must be kept confidential. Article 14(1)(28) of the P2SK Law provides: "Bank secrecy is everything relating to information concerning depositors and their deposits". Legally, the provisions on banking secrecy are set forth in Article 37 (1) and (2) of the P2SK Law, which stipulate that banks must maintain the confidentiality of information concerning depositors and their deposits. Even if a depositor also serves as a borrower, the bank and its affiliated parties remain obligated to keep confidential any information relating to the customer in their capacity as a depositor. Exceptions to these requirements do exist, and the specific conditions for those exceptions are expressly detailed in Articles 38 through 47 of the P2SK Law.

However, if we examine the historical development of banking in Indonesia, the history of banking secrecy can be divided into two periods:

i. **Pre-1998 Banking Law period:** During this period, the concept of banking secrecy was interpreted broadly to include depositors, borrowers, and other users of banking services.
ii. **Post-1998 Banking Law period:** After the 1998 Banking Law came into effect, banking secrecy was defined more narrowly, applying only to depositors and their deposited funds.

The enactment of the 1998 Banking Law reflected changes that were partial yet fundamentally significant. One of the key aspects revised and refined was the provision on bank secrecy, which was judged capable of accommodating the broader public's demand for updated rules governing banking confidentiality. As noted in the eighth paragraph of the general commentary, the amendment of bank-secrecy provisions was tied to

efforts to strengthen social control over banking institutions. The core change introduced by the 1998 Banking Law, compared to the previous regime, was the need to reassess the overly stringent and opaque nature of existing secrecy rules. Consequently, although bank secrecy remains an essential element for any institution entrusted with public funds, the 1998 Banking Law provides that not all facets of a bank's operations must be kept entirely confidential.

The interrelationship between banking secrecy and customers' personal data can be examined in terms of both substance and protection mechanisms. As previously discussed, through the broadened definition in the P2SK Law, banking secrecy in principle also encompasses customers' personal data. However, not all personal data qualifies as banking secrets. Under the Personal Data Protection Law, a bank is classified as a data controller—i.e., an entity authorized to determine the purposes of and exercise control over the processing of personal data. This aligns with Article 1(4) of the Personal Data Protection Law, which states: *"A Personal Data Controller is any individual, public body, or international organization acting alone or jointly in determining the purposes of and exercising control over the processing of Personal Data".*

According to Article 1(1) of the Personal Data Protection Law, personal data is any information concerning a person who is identified and/or can be identified, either directly or indirectly, through combination with other information, by means of electronic and/or non-electronic systems

On the other hand, in the banking context, although the term 'personal data' is not explicitly mentioned, the concept of customer information confidentiality—as previously described—is stipulated in Article 37 of the P2SK Law, which requires banks to safeguard the confidentiality of all information related to their customers, including identity data and financial information.

3.2 Types of Personal Data That Are Protected

The classification of data covered by the Personal Data Protection Law is divided into two categories—'specific personal data' and 'general personal data'—as set forth in Article 4 of that law. When mapped to the types of data within the scope of the P2SK Law, these categories can be further detailed as provided in Article 19 of Financial Services Authority Regulation No. 22 of 2023 on Consumer and Community Protection in the Financial Services Sector.

In these provisions, "Consumer Personal Data and/or Information" refers to data and/or information that includes the following:

a. Individuals:

1. Name.
2. Address.
3. Date of birth and/or age.
4. Telephone number.
5. Mother's maiden name.

b. Corporations:

1. Name.
2. Address.
3. Telephone number.
4. Composition of the board of directors and commissioners, including identity documents such as national ID card, passport, or residence permit.
5. Composition of shareholders.

Referring to the provisions of the Personal Data Protection Law and the P2SK Law, the types of bank customers' personal data that must be kept confidential can be organized as shown in the following table:

No.	Data Protected under the Personal Data Protection Law	Banking Secrecy Data under the P2SK Law.	Remarks
1.	**Full name** Article 4(3)(a)	**Customer identity** Article 14(1)(37)	Both protect personal identity information.
2.	**Identity numbers** (NIK, passport number, NPWP) Article 4(3)(f)	**Account number & account holder name** Article 14(1)(37)	Administrative identifiers that must be kept confidential.
3.	**Address, email, telephone number** Article 4(3)(f)	Part of customer identity.	Customer contact details are confidential and must be protected by the Data Controller..

4.	**Financial & account information** Article 4(2)(f)	**Account balances, transaction history, financial transactions** Article 14(1)(37)	Financial data is expressly protected and must be secured by the Data Controller.
5.	**Biometric data** (fingerprint, facial recognition) Article 4(2)(b)	Not explicitly listed.	Usage governed by the Personal Data Protection Law's general provisions.
6.	**Location data & digital-activity logs** Article 4(3)(f)	Not explicitly listed	Usage governed by the Personal Data Protection Law's general provisions.
7.	**Dependency/family information** Article 4(2)(e)	Not explicitly listed	Usage governed by the Personal Data Protection Law's general provisions.
8.	**Digital-account credentials** (password, user ID) Article 4(2)(f)	**Customer system-access data.** Article 14(1)(37)	Protection of customer account access is mandatory under banking-secrecy rules.

From the foregoing descriptions in the table, the types of customer personal data that banks—acting as data controllers—must protect are:

No.	Customer Personal Data	Description	Legal Basis
1.	Full Name	Includes the customer's complete legal name, place and date of birth, gender, nationality, and marital status. Classified as general personal data.	Personal Data Protection Law No. 27/2022, Art. 4 (3) (a). P2SK Law No. 4/2023, Art. 14 (1) (37).
2.	National Identity numbers and official documents.	Includes NIK (national ID number), passport number, driver's license (SIM), NPWP, or other identifying documents.	Personal Data Protection Law No. 27/2022, Art. 4 (3) (f).
3.	Contact Data.	Includes the customer's address, telephone number, email, and social-media accounts used for communication with the bank.	Personal Data Protection Law No. 27/2022, Art. 4 (3) (f).
4.	Location data & digital-activity logs.	The customer's location when accessing banking services, as well as usage logs from mobile-banking or internet-banking applications. These're critical for securing online transactions in the digital era.	Personal Data Protection Law No. 27/2022, Art. 4 (3) (f).
5.	Family or dependency data.	Information regarding the customer's spouse, children, or heirs.	Personal Data Protection Law No. 27/2022, Art. 4 (2) (e).
6.	Digital-access cerdentials	Consists of user ID, password, PIN, OTP code, and the devices used to access digital banking services.	Personal Data Protection Law No. 27/2022, Art. 4 (2) (f).

3.3 Protection of Bank Customers' Personal Data

The Personal Data Protection Law, functioning as a **Lex Habeas Data**, in Article 3 sets forth several legislative principles that form the foundation for data-protection implementation in Indonesia. These principles include protection legal certainty, public interest, utility, prudence, balance, accountability, confidentiality all of which aim to guarantee respect for every individual's right to privacy and the protection of their personal data. *Lex Digitalis Habeas Data* is based on the concept of personal-data-protection legal subjects who carry out data-protection legal acts and incur legal consequences for protecting personal data in activities that connect, interact with, and transact digital data in cyberspace/virtual environments.

Legal protection, as referred to in this context, relates to the ability of the interested party to effectively enforce the rights granted to it. An 'interested party' means an individual or legal entity whose interests are directly affected by a decision issued by a governmental body. In legal doctrine, there are several forms of legal protection, namely as follows:

1) Juridical Legal Protection.

A form of protection that is regulated and established in legislation and enforced through applicable

procedures.

2) Practical Legal Protection.

In criminal-law enforcement practice, practical legal protection begins once a case is reported to the police. This protection is granted impartially to both the complainant and the accused. Generally, it adheres to existing legal norms and is intended to ensure procedural justice. Thus, practical legal protection can be understood as safeguarding the rights and interests of legal subjects throughout law enforcement and dispute-resolution processes.

3) Preventive Legal Protection.

Within administrative law, preventive legal protection serves as a forum for the public to submit objections (inspraak) or opinions before a government decision is finalized. It can be described as measures—either enshrined in legislation or agreed upon in preventive contracts—designed to protect the rights and interests of legal subjects, prevent violations, and define the boundaries of obligations.

Legal protection for bank customers' personal data is also grounded in the principles of justice and legal certainty as mandated by the Constitution and statutory regulations. The enactment of the Personal Data Protection Law and the Banking Law further underscore the bank's duty to safeguard the confidentiality and integrity of personal data. As legal subjects, customers possess the right to information, the right to data correction, and even the right to be forgotten ("right to be forgotten") as part of their control over their personal information. The Financial Services Authority requires financial institutions to obtain consumers' explicit consent before collecting, storing, or using their personal data. Any processing of data without consent or misuse beyond the agreed purpose constitutes a breach of consumer-protection principles and may attract administrative sanctions. This is in line with the principles of purpose limitation and access limitation.

Financial Services Authority Regulation No. 22 of 2023 on Consumer and Community Protection in the Financial Services Sector mandates additional safeguards, including the obligation for financial service providers to establish a complaint mechanism in the event of data misuse. Consumers have the right to request correction, erasure, or restriction of the processing of their personal data. In the event of a data breach, the financial institution must report it to the Financial Services Authority and notify all affected consumers at the earliest opportunity. This measure represents the institution's legal and moral responsibility for any harm resulting from negligence or cyberattacks.

To support the effectiveness of these regulations, the Financial Services Authority (OJK) conducts periodic oversight and examinations of financial institutions and promotes the reporting of information-security incidents through an integrated reporting system. If any violations are identified—pursuant to FSA Regulation No. 22 of 2023 and FSA Regulation No. 44 of 2024—the OJK may impose sanctions ranging from written warnings and business- activity restrictions to the revocation of operating licenses. Consequently, customer-data protection under OJK rules is not merely a normative requirement but an operational imperative. These regulations establish a robust, comprehensive legal framework to ensure that customers' personal data are protected from misuse by both internal and external actors. The OJK's dual role as regulator and supervisor embeds data protection as an inseparable element of responsible, consumer-oriented governance in the financial-services sector.

Data and information protection are explicitly codified in Article 19 of OJK Regulation No. 22/2023 on Consumer and Community Protection in the Financial Services Sector. Under Article 19, Financial Service Providers must safeguard the security and confidentiality of consumers' personal data, use that data solely for purposes and objectives consented to by the consumer, provide product and/or service information in a clear, non-misleading manner and btain consumer consent before accessing or using personal data. As data controllers and Financial Service Providers, banks are obliged to ensure that their information systems and cyber-resilience measures are optimally implemented to protect customers. Under Article 24(2) of OJK Regulation No. 22/2023, they must establish information-security safeguards that guarantee the confidentiality, integrity, and availability of managed data and information, effectively and efficiently, in full compliance with applicable laws. These safeguards encompass technological controls (e.g., network security, encryption), human-resource management (e.g., staff training, access controls), and process controls (e.g., change management, incident-response procedures).

Furthermore, the obligation of banks to safeguard customers' personal data is also governed by Financial Services Authority Regulation No. 44 of 2024 on Banking Secrecy. Conversely, certain exceptions to these confidentiality duties—triggered by specific conditions—are explicitly set forth in the same regulation. Article 3 delineates the limited circumstances under which a bank may lift its duty to maintain the secrecy of depositor and investor information, including their deposits and investments. In implementing these provisions, banks are required to establish formal procedures for invoking banking-secrecy exceptions and to document all requests for, and disclosures of, confidential banking information.

Financial Services Authority Regulation No. 22 of 2023, together with Regulation No. 44 of 2024, represents strategic measures taken by the Financial Services Authority to reinforce the protection of

customers' personal data in the financial services sector. By establishing consumer-protection principles and prescribing obligations for Financial Service Providers, these regulations are expected to foster a secure and trustworthy financial ecosystem. Consistent implementation and rigorous oversight are key to ensuring that consumers' rights remain guaranteed and that public confidence in the financial sector is continuously upheld.

4 CONCLUSION.

Based on the foregoing explanation, it can be concluded that the instruments for protecting bank customers' personal data in Indonesia's financial system have been established to ensure the fulfillment of customers' rights. These instruments are embodied in the Personal Data Protection Law and the P2SK Law and are further reinforced by implementing regulations that operationalize their principle, such as Financial Services Authority Regulation No. 22 of 2023 on Consumer and Community Protection in the Financial Services Sector and Regulation No. 44 of 2024 on Banking Secrecy. The interconnection of these four regulations plays a crucial role as a bridging mechanism to strengthen banks' safeguarding of customers' personal-data confidentiality, which principally includes:

1. Protection of depositors' assets, privacy, and data (including investors and their investments) as a core principle of safeguarding financial-services users.
2. Banks are obliged to maintain the confidentiality of their customers' personal data, ensure transparency in data handling toward data subjects (i.e., the account holders), and to preserve and enhance the integrity of all personnel and affiliates involved.
3. Banks must obtain clear and unequivocal consent from consumers before using or processing personal data and are responsible for securing those data against unauthorized access or potential misuse.
4. Administrative sanctions apply to banks that fail to meet these obligations—ranging from written warnings and business-activity restrictions to fines, license revocation, and, where legal violations occur, criminal penalties.

For the mutual benefit of both banks and customers—who both seek to achieve profitable outcomes—the collaboration among regulators, industry participants, and the public regarding customers' personal data is key. The protection of customers' personal data is not merely a legal obligation but also an element of sound governance and an effort to build public trust in the national financial system. Therefore, it is essential for every banking institution to strictly comply with these provisions and to cultivate a data-protection culture as part of delivering exemplary service to customers as consumers.

LEGISLATION REFERENCE

[1] The 1945 Constitution of the Republic of Indonesia. Law No. 27 of 2022 on Personal Data Protection.
[2] Law No. 4 of 2023 on the Development and Strengthening of the Financial Sector. Financial Services Authority Regulation No. 22 of 2023 on Consumer Protection. Financial Services Authority Regulation No. 44 of 2024 on Banking Secrecy.

BOOK

[3] Budhijanto, Danrivanto. 2023. *The Law of Personal Data Protection in Indonesia: Cyberlaw and Cybersecurity*. PT. Refika Aditama, Bandung.
[4] Sri Agustina, Rani. 2017. *Banking Secrecy*. CV. Keni Media, Bandung. Marzuki, Peter Mahmud. 2007. *Legal Research*. Kencana, Jakarta.

[5] Ramli, Ahmad M. 2023. *The Personal Data Protection Law and Corporations: Discussion of Current Issues in Law No. 27 of 2022 on Personal Data Protection*. PT. Refika Aditama, Bandung.
[6] Zamroni, M. 2024. *Compendium of Legal Theories & Legal Concepts for Legal Research*. Scopindo Media Pustaka, Surabaya.

JOURNAL

[7] Daya Negri Wijaya. 2016. "The Social Contract According to Thomas Hobbes and John Locke." *Journal of Humanist Educational Sociology* 1, no. 2 (December 2016). Department of History, Universitas Negeri Malang.