Legal Protection Efforts for Customer Rights in Cases of Personal Data Breaches in Banking

Aisyah Maulani[1], Agustianto[2], Risno Mina[3], Ratna Kumala Sari[4], John Elvin Louis[5]

[1-2]Faculty of Law, Universitas Internasional Batam, Indonesia
[3]Faculty of Law, Universitas Muhammadiyah Luwuk-Banggai, Indonesia
[4]Faculty of Law, Universitas Sang Bumi Ruwa Jurai, Indonesia
[5]Faculty of Law, Youngsan University, South Korea
Corresponding email: agustianto.lec@uib.ac.id

History of Article
Submitted : March 16, 2026
Revised : May 22, 2026
Accepted : June 01, 2026
Published : June 23, 2026
DOI : https://doi.org/10.37253/barjoules.v4i1.12406

Abstract

In the rapidly evolving digital era, banking activities increasingly rely on electronic systems and online services. Behind this convenience lies a significant risk concerning the protection of customers' personal data. This article examines the legal protection of customers' rights in the event of personal data breaches by banking institutions. The study employs a mixed-method approach (normative and empirical). The normative approach involves analyzing relevant legal instruments such as Law Number 27 of 2022 on Personal Data Protection, Law Number 10 of 1998 on Banking, and regulations issued by the Financial Services Authority (OJK). The empirical aspect is supported by interviews with bank staff in the compliance and customer service divisions to understand how these regulations are applied in practice. The findings reveal that while the legal framework is relatively comprehensive, its implementation remains problematic. Issues include low legal literacy among customers, limited public outreach by banks, and technical constraints in countering the rapidly evolving cyber threats. Banks hold legal, ethical, and technical responsibilities to protect data and must provide compensation when negligence occurs. Dispute resolution mechanisms include internal complaints, mediation through OJK, or civil litigation. The study recommends the establishment of an independent supervisory body, the enhancement of public education on data rights, and the strengthening of internal bank security systems to ensure long-term customer data protection.

Keywords: Legal Protection, Customer Rights, Data Breach, Banking, Personal Data Protection

Introduction

In the digital era, banking and financial activities are increasingly carried out through online systems, including transactions, account opening, loan applications, and mobile banking services. This development provides convenience for customers, but it also creates new risks related to the protection of personal data. The use of digital banking services requires stronger legal safeguards because customer data may be exposed to misuse, unauthorized access, and cybercrime (Ayunda & Rusdianto, 2021). Recently, public concern has increased due to several data breach cases involving financial institutions and digital service providers.

Customer data breaches are not a trivial matter. Leaked data may be misused for fraud, identity theft, illegal access to accounts, and other forms of cybercrime. These risks may cause material losses, psychological harm, and a decline in public trust toward banking institutions. Data breaches in digital banking can create serious consequences for customers, especially when sensitive information is accessed and distributed without authorization (D. F. Putri et al., 2023). In Batam City, which continues to develop as a digital-based economic area, this issue becomes more relevant because many people depend on online banking services.

As a form of legal protection, Indonesia has enacted Law Number 27 of 2022 concerning Personal Data Protection. This law strengthens the legal position of individuals as personal data subjects and provides a clearer basis for protecting personal data in digital activities. In the banking sector, customer protection is also closely related to the obligation of banks to maintain the confidentiality of customer information. However, the existence of legal instruments does not automatically guarantee effective implementation, especially when public legal awareness and institutional readiness remain limited (Fikri & Rusdiana, 2023).

Several data breach cases in Indonesia show that the protection of customer data still faces serious challenges. One of the cases that attracted public attention was the data breach involving Bank Syariah Indonesia, where customer data was allegedly stolen and distributed by a hacker group. This incident shows that digital banking systems remain vulnerable to cyberattacks and that banks must

strengthen their responsibility in protecting customer data. In this regard, That banks may bear legal responsibility when customer data is leaked, particularly when the breach is related to negligence or weak data protection systems (Annafa et al., 2024).

Normatively, customer data protection in Indonesia has been regulated through several legal instruments. Article 40 of Law Number 10 of 1998 concerning Banking requires banks to maintain the confidentiality of information regarding depositors and their deposits. Meanwhile, the Personal Data Protection Law requires personal data processing to be carried out lawfully, fairly, transparently, and with respect for the rights of data subjects. Although mobile banking provides convenience for customers, it also increases the risk of personal data misuse if legal protection and security systems are not implemented effectively (Irmawati et al., 2024).

However, legal protection for customer data is still not fully optimal in practice. Many customers do not understand the available complaint mechanisms or the legal remedies that can be taken when their personal data is leaked. In addition, banks and financial institutions still face challenges in strengthening cybersecurity systems, improving internal supervision, and providing clear recovery mechanisms for customers. This condition shows that data protection is not only a regulatory issue, but also an issue of institutional accountability and public legal awareness (Anbiya & Januarita, 2026).

Previous studies have discussed various aspects of personal data protection. (Rahmawati et al., 2023) highlight the importance of bank accountability in cases of customer data breaches, while (D. D. F. Putri & Fahrozi, 2021) discuss the urgency of preventing consumer data breaches through stronger personal data protection regulations. (Delpiero et al., 2021) also show that digital platform accountability remains an important issue in personal data protection. However, these studies have not fully examined the effectiveness of legal protection for customer rights in banking data breach cases, especially in relation to recovery mechanisms for harmed customers.

Given the increasing number of data breach cases that cause public concern and can lead to both financial and psychological harm, the author considers it

important to raise this issue in research. The main focus of this research is to answer several questions, such as: to what extent are the laws and regulations, particularly the PDP Law, effective in protecting customer rights; what forms of legal protection and remedies can be obtained by customers after a data breach; and what are the mechanisms for the recovery of rights for customers who have suffered losses.

This study aims to analyze the effectiveness of the PDP Law and identify the legal measures that can be taken by customers who fall victim to data breaches. It is expected that this research can serve as legal literature as well as a guide for the public to better understand their rights and know what to do if their data is leaked. The limitation of this research lies in its scope, which focuses solely on the banking sector and does not cover other financial institutions such as fintech or insurance. This topic was chosen because the protection of customer rights amid data breach threats is a crucial issue that is often overlooked, even though it is closely related to public trust in the ever-growing digital banking sector.

Research Method

This research employs a mixed legal research method by combining normative juridical and empirical juridical approaches. The normative juridical approach is used to examine the legal framework governing customer data protection in the banking sector. This examination focuses on legal norms related to personal data protection, electronic transactions, banking supervision, consumer protection, and constitutional rights. Meanwhile, the empirical juridical approach is used to understand how these legal norms are implemented in banking practice (Tan, 2021). This approach is carried out by examining the experiences and perspectives of bank employees regarding customer data protection, institutional supervision, and the handling of potential data breaches. The use of a mixed method is relevant because this research does not merely analyze the substance of legal norms, but also evaluates their practical application. The approaches used in this research include statutory, conceptual, and empirical approaches. The statutory approach examines relevant legal instruments, while

the conceptual and empirical approaches are used to analyze legal concepts and their implementation in banking institutions (Disemadi, 2022).

The data used in this research consist of primary data and secondary data. Primary data were obtained through interviews with two bank employees from different branches within the same banking institution. These interviews were conducted to obtain practical information regarding the implementation of customer data protection, internal banking procedures, preventive measures against data breaches, the supervisory role of the Financial Services Authority (OJK) and Bank Indonesia (BI), and the bank's responsibility in providing remedies or compensation when violations occur. Secondary data consist of legal materials, which include primary, secondary, and tertiary legal materials. Primary legal materials include the 1945 Constitution, Law Number 27 of 2022 on Personal Data Protection, the Law on Electronic Information and Transactions, the Consumer Protection Law, OJK regulations, BI regulations, and other relevant laws and regulations. Secondary legal materials include books, journal articles, research reports, legal doctrines, and scholarly opinions related to personal data protection, banking law, consumer protection, and digital security, while tertiary legal materials include legal dictionaries and other supporting references. Data collection was conducted through literature study and interviews to obtain both normative and empirical information. All data were analyzed qualitatively using a descriptive-analytical method by interpreting legal norms, comparing them with empirical findings, and assessing the effectiveness of legal protection for customers' rights in cases of data breaches (Antony et al., 2026).

Results and Discussions

Regulations Regarding the Protection of Customer Rights in Indonesia

The protection of customer rights in Indonesia is regulated through several legal instruments that are closely connected to banking law, personal data protection, consumer protection, and electronic transaction law. In the banking

sector, customer protection is inseparable from the obligation of banks to maintain the confidentiality, security, and lawful use of customer information (Katiandagho et al., 2023). This protection becomes increasingly important because banking services are no longer limited to conventional transactions, but have expanded into mobile banking, internet banking, digital payments, and electronic financial services. The development of digital banking creates convenience for customers, yet it also increases the risk of data leakage, unauthorized access, identity misuse, and cybercrime. Therefore, customer data must be understood not only as banking information, but also as personal data that is attached to the legal rights of individuals (Nasution, 2025). The protection of customer rights must be placed within a broader legal framework that combines privacy, consumer protection, financial supervision, and institutional responsibility. This shows that customer protection in Indonesia requires an integrated regulatory approach rather than a sectoral and fragmented understanding.

The main legal basis for personal data protection in Indonesia is Law Number 27 of 2022 concerning Personal Data Protection. This law provides a more comprehensive framework for protecting personal data by regulating the principles of data processing, the rights of data subjects, the obligations of data controllers and data processors, data transfer, administrative sanctions, dispute resolution, and criminal provisions (Fikri & Rusdiana, 2023). In the context of banking, customers may be regarded as data subjects whose personal data are collected, stored, processed, and used by banks in providing financial services. The bank, in this position, may act as a data controller because it determines the purpose and method of processing customer data (Algamar & Ismail, 2023). The Personal Data Protection Law is important because it shifts the protection of customer data from a purely administrative obligation into a legal right that must be respected and enforced. It also provides a stronger legal foundation for customers to demand accountability when their personal data are unlawfully used or inadequately protected. Thus, the law strengthens the position of customers in facing the risk of data breaches in the financial services sector (Wibowo et al., 2024).

Customer rights under the Personal Data Protection Law include the right to obtain information, access personal data, correct inaccurate data, withdraw consent, request deletion, and object to certain forms of data processing. These rights are highly relevant in the banking sector because customers often provide sensitive information, such as identity data, financial records, contact details, transaction history, and other information required for financial services violated (Purnama & Alhakim, 2021). The processing of such data must be based on lawful grounds and must be carried out transparently, proportionally, and securely. Consent is an important element because customers must understand how their data will be collected, used, stored, shared, or transferred. However, consent should not be treated merely as a formal clause in banking documents, but as a substantive expression of the customer's control over personal information. Banks must also ensure that the processing of customer data is limited to legitimate banking purposes and does not exceed what is necessary (B. M. L. Putri et al., 2025). Therefore, customer rights protection requires both legal compliance and ethical responsibility in the management of personal data.

The protection of customer data is also regulated under Law Number 10 of 1998 concerning the Amendment to Law Number 7 of 1992 concerning Banking. One of the central principles in banking law is bank secrecy, which requires banks to protect information concerning depositors and their deposits. This obligation reflects the trust-based nature of banking relationships, where customers rely on banks to manage their financial information responsibly (Bodhi & Tan, 2022). Bank secrecy is not merely a technical rule, but a fundamental principle that supports public confidence in the banking system. If customer information is disclosed or misused without lawful basis, the credibility of banking institutions may be seriously affected. However, bank secrecy must now be interpreted together with the broader framework of personal data protection because customer information is not limited to deposit data alone (Algamar et al., 2024). Therefore, the obligation to maintain bank secrecy should be expanded in practice to include stronger digital security, responsible data processing, and protection against unauthorized access.

E-ISSN: 3026-3182
Available online at website: https://journal.uib.ac.id/index.php/barjoules/index

The role of the Financial Services Authority is also important in protecting customer rights in the financial services sector. Through OJK regulations on consumer and community protection in the financial services sector, financial service providers are required to uphold principles such as transparency, fair treatment, responsible business conduct, consumer education, complaint handling, and dispute resolution (Annafa et al., 2024). These principles are relevant because customers are often in a weaker position compared to financial institutions in terms of information, bargaining power, and technical understanding. In the context of customer data protection, OJK supervision is needed to ensure that banks do not only provide financial products, but also maintain adequate governance over customer information. Customer protection must therefore include preventive measures, internal control, risk management, and effective response mechanisms when violations occur (Chairunnisa et al., 2024). Complaint mechanisms are particularly important because customers need accessible channels to report losses caused by data breaches or misuse of information. Thus, OJK regulations strengthen the institutional dimension of customer rights protection in Indonesia.

Bank Indonesia also plays an important role in consumer protection, especially in relation to payment systems and financial services under its authority. Bank Indonesia regulations concerning consumer protection emphasize legal certainty, protection of consumer data and information, protection of consumer assets, responsible business conduct, education, transparency, and effective complaint handling (Shahrullah et al., 2024). These provisions are relevant to digital banking because many banking transactions are connected to electronic payment systems, payment service providers, and digital financial infrastructure. In practice, customer protection in digital transactions requires coordination between banks, payment system operators, Bank Indonesia, and other relevant authorities. Bank Indonesia's regulatory framework complements the role of OJK by focusing on the stability, security, and reliability of payment systems. This is important because data breaches in digital payment services may directly affect customer funds, transaction security, and public trust (Munawaroh et al., 2025). Therefore, the protection of customer

rights in Indonesia must be understood as a shared responsibility between banking institutions, supervisory authorities, and payment system regulators.

Customer rights protection is also connected to the Law on Electronic Information and Transactions, as amended most recently by Law Number 1 of 2024. This regulation is relevant because banking services increasingly operate through electronic systems and digital platforms. Banks that provide mobile banking, internet banking, and other electronic services must ensure that their systems are reliable, secure, and capable of protecting electronic information (Setiawan & Najicha, 2022). In this context, customer data protection is not only a matter of banking confidentiality, but also part of electronic system governance. Security failures in banking platforms may create legal consequences when they result in unauthorized access, manipulation, loss, or misuse of customer data. Therefore, legal protection must include both preventive obligations and remedial mechanisms after a data breach occurs (Antony et al., 2025). The interaction between the Personal Data Protection Law and the Electronic Information and Transactions Law strengthens the legal basis for protecting customers in the digital banking environment (Weley & Disemadi, 2022).

Civil law also provides an important legal basis for customer protection when data breaches cause material or immaterial losses. Article 1365 of the Indonesian Civil Code concerning unlawful acts may be used as a basis for compensation claims when a party suffers losses due to the fault or negligence of another party. In cases of customer data breaches, this provision may be relevant if the bank fails to implement adequate security measures, neglects its duty of care, or allows unlawful disclosure of customer information (Bodhi & Tan, 2022). The customer may argue that the bank's negligence constitutes an unlawful act when it causes financial loss, reputational harm, psychological distress, or other forms of damage. Material losses may include unauthorized transactions, financial fraud, or expenses incurred to recover from identity misuse. Immaterial losses may include anxiety, reputational damage, and loss of trust caused by the exposure of personal information (Manurung et al., 2025). Therefore, civil liability functions as a corrective mechanism to ensure that

E-ISSN: 3026-3182
Available online at website: https://journal.uib.ac.id/index.php/barjoules/index

customer rights are not only protected by regulation, but also enforceable through compensation.

At the international level, the General Data Protection Regulation of the European Union is often used as a comparative reference in strengthening personal data protection. The GDPR emphasizes principles such as lawfulness, fairness, transparency, purpose limitation, data minimization, accuracy, storage limitation, integrity, confidentiality, and accountability (Widjaja, 2026). These principles are relevant for Indonesia because they provide a more mature model of data governance and institutional accountability. The GDPR also recognizes the importance of breach notification, data subject rights, and obligations of data controllers and processors (Algamar et al., 2024). Indonesia's Personal Data Protection Law has adopted several similar principles, but its effectiveness depends on consistent enforcement, technical implementing regulations, institutional readiness, and public awareness. In the banking sector, comparison with the GDPR shows that customer data protection must be supported by clear procedures, strong security standards, and effective supervision. Therefore, international standards can serve as a reference for improving the implementation of customer rights protection in Indonesia (Arbain et al., 2026).

In Batam City, the protection of customer rights has particular significance because the city continues to develop as an industrial, investment, and digitally connected economic area. The growth of business activities, cross-border mobility, and digital transactions increases the use of banking services and electronic payment systems (Azza & Taek, 2025). This situation makes customer data increasingly valuable and vulnerable to misuse by irresponsible parties. The risk of cybercrime, fraud, phishing, unauthorized access, and digital identity theft must therefore be anticipated through stronger regulatory compliance and institutional supervision. Banks operating in Batam must ensure that customer data protection is implemented not only at the central policy level, but also at the branch and operational levels. Local implementation is important because customers often interact directly with branch offices, banking officers, and digital service channels in their daily transactions. In conclusion, the regulation of customer rights protection in Indonesia already has a relatively strong legal

foundation, but its effectiveness depends on consistent enforcement, institutional accountability, technological readiness, and the ability of banks to protect customers in real practice (Ahmad et al., 2025).

The Effectiveness of Personal Data Protection in Safeguarding Customer

The effectiveness of personal data protection in safeguarding customers in the banking sector can be analyzed through Soerjono Soekanto's theory of legal effectiveness. This theory explains that the effectiveness of law is influenced by five main factors, namely legal substance, law enforcement, facilities, society, and legal culture. These five factors are relevant because the protection of customer data does not depend only on the existence of written regulations. It also depends on how those regulations are enforced, supported by institutional capacity, understood by society, and internalized as part of legal culture (Judijanto et al., 2024). In the banking sector, personal data has a highly sensitive character because it is directly connected to identity, financial transactions, account ownership, and customer trust. Therefore, the effectiveness of personal data protection must be measured not only from normative availability, but also from its practical ability to prevent, respond to, and remedy data breaches (Shahrullah et al., 2024). Based on this framework, customer protection in Indonesia must be understood as a combination of legal regulation, institutional accountability, technological readiness, and public awareness.

From the perspective of legal substance, Indonesia already has several legal instruments that provide a normative basis for protecting customer data. Law Number 27 of 2022 concerning Personal Data Protection establishes the rights of data subjects, the obligations of data controllers and data processors, and the principles of lawful personal data processing. In the banking context, this law is important because banks collect and process customer data in almost every financial service activity (Yuspin et al., 2023). In addition, the Banking Law requires banks to maintain the confidentiality of information related to customers, particularly depositors and their deposits. OJK regulations on

consumer and community protection in the financial services sector also strengthen the obligation of financial service providers to protect consumers fairly, transparently, and responsibly (Rosadi et al., 2023). These regulations show that customer data protection in Indonesia has a relatively strong legal foundation. However, legal substance alone is not sufficient if the norms are not followed by clear technical standards, consistent supervision, and effective enforcement.

The Personal Data Protection Law marks an important development in Indonesia's legal framework because it places personal data as a legal right attached to individuals. Through this law, customers are no longer viewed merely as users of banking services, but also as data subjects who have control over their personal information (Silviani et al., 2023). This position gives customers the right to obtain information, access data, correct inaccurate data, withdraw consent, request deletion, and seek remedies when their data is misused. In the banking sector, these rights are essential because customer data may include identity numbers, addresses, phone numbers, transaction histories, account balances, and other confidential financial information. If such data is leaked or misused, the losses suffered by customers may be both material and immaterial (K. D. Kurniawan et al., 2024). Material losses may arise from unauthorized transactions, fraud, or identity theft, while immaterial losses may include anxiety, reputational harm, and loss of trust. Therefore, the effectiveness of the Personal Data Protection Law depends on whether these rights can be implemented in real banking practices.

The increasing use of mobile banking and digital financial services creates new challenges for the effectiveness of personal data protection. Digital banking enables customers to conduct transactions more easily, but it also expands the potential points of vulnerability in the financial system (Wang et al., 2024). Personal data may be exposed through phishing, hacking, malware, social engineering, weak authentication systems, or negligence in internal data management. This condition shows that legal protection must be accompanied by technical security measures that are capable of responding to rapidly changing digital risks. As stated by Irmawati et al., 2024, the development of mobile

banking increases the risk of personal data misuse when legal protection is not supported by effective implementation. This means that regulation must be translated into operational policies, cybersecurity standards, employee discipline, and incident response mechanisms (Cele & Kwenda, 2025). Without effective implementation, personal data protection may remain a formal legal obligation without meaningful protection for customers.

Law enforcement is the second factor that determines the effectiveness of personal data protection in the banking sector. Institutions such as the Financial Services Authority, Bank Indonesia, and internal compliance units within banks have important roles in supervising the implementation of customer protection (Waliullah et al., 2025). OJK is responsible for supervising financial service institutions, ensuring consumer protection, and requiring banks to provide complaint handling mechanisms. Bank Indonesia also has authority in relation to payment systems and consumer protection within the scope of its regulatory functions (Sulistyandari & Sutrisno, 2023). In addition, internal compliance units are expected to ensure that banks comply with legal obligations, internal policies, and risk management standards. When data breaches occur, law enforcement must be able to identify responsibility, determine sanctions, and ensure that customers receive proper remedies (Sriono et al., 2024). Therefore, effective law enforcement requires coordination among regulators, banking institutions, and complaint resolution mechanisms.

Bank accountability becomes a central issue when customer data is leaked, misused, or accessed without authorization. Banks have a duty to protect customer information because the relationship between banks and customers is built on trust, confidentiality, and professional responsibility. If a breach occurs due to weak security systems, negligence, inadequate supervision, or failure to comply with legal obligations, the bank may be held responsible. Emphasize that customer data breaches may cause material and immaterial losses, making institutional accountability necessary (Rahmawati et al., 2023). Accountability should not only be understood as the imposition of sanctions, but also as the obligation to provide clarification, assistance, recovery, and compensation to affected customers. In this context, the effectiveness of legal protection depends

on whether customers have practical access to complaint channels and remedies. If compensation mechanisms are unclear or difficult to access, the protection of customer rights becomes less effective in practice (D. A. Kurniawan et al., 2024).

The third factor in legal effectiveness is the availability of facilities and infrastructure to support the implementation of the law. In the banking sector, these facilities include cybersecurity systems, encryption technology, secure authentication, internal monitoring systems, audit mechanisms, and data breach response procedures (Rumbruren & Watofa, 2025). Banks must also provide regular employee training because many data breaches may occur not only due to technological weaknesses, but also due to human error or lack of awareness. Strong infrastructure is necessary to ensure that customer data is protected from unauthorized access, manipulation, disclosure, or destruction. Complaint channels must also be accessible, transparent, and responsive so that customers can report suspicious transactions or data misuse quickly. D. F. Putri et al., 2023 show that data breach cases in digital banking may create serious risks when personal information is accessed and misused without authorization. Therefore, facilities and infrastructure are essential elements in transforming legal norms into actual protection.

The fourth factor is society, particularly the level of customer awareness regarding personal data protection. Customers play an important role in protecting their own data because many digital banking risks are connected to user behavior (Yuspin et al., 2024). For example, customers may become victims of phishing or social engineering when they unknowingly disclose passwords, one-time passwords, personal identification numbers, or other confidential information. However, customer awareness cannot be separated from the responsibility of banks to provide education, warnings, and clear information regarding digital security. Legal protection will be more effective when customers understand their rights, recognize risks, and know the steps to take when their data is misused. Public awareness also strengthens the demand for accountability because informed customers are more likely to report violations and seek remedies (Alrawhani et al., 2025). Therefore, the effectiveness of personal data

protection requires cooperation between legally responsible institutions and customers as active participants in digital security.

The fifth factor is legal culture, which refers to the values, attitudes, and habits that influence how law is understood and practiced. In the context of personal data protection, legal culture requires a shift in perspective from viewing customer data as mere administrative information to recognizing it as part of privacy and consumer rights (Johri & Kumar, 2023). This shift is important because weak legal culture may cause banks, employees, and customers to underestimate the seriousness of data protection obligations. D. D. F. Putri & Fahrozi, 2021 argue that stronger personal data protection regulation is needed to prevent consumer data breaches in digital transactions. Although this view was expressed before the enactment of the Personal Data Protection Law, it remains relevant because the challenge today lies in implementation and compliance (Nagari & Raharja, 2025). Banks must develop a culture of accountability, confidentiality, transparency, and respect for customer rights. Without a strong legal culture, even comprehensive regulations may fail to provide effective protection.

The effectiveness of personal data protection also depends on the integration between legal norms, regulatory supervision, and institutional governance. The Personal Data Protection Law provides the general framework, while banking regulations and consumer protection rules provide sectoral obligations for financial service providers (Nurkholisah et al., 2025). This layered regulatory structure is important because customer data protection in banking involves both privacy rights and financial consumer protection. However, regulatory overlap may also create challenges if coordination between institutions is weak or if banks face uncertainty regarding reporting, supervision, and complaint handling obligations (Widiatedja & Mishra, 2023). For this reason, the roles of OJK and Bank Indonesia must be harmonized with the broader personal data protection framework. Banks must also establish internal governance systems that clearly regulate data processing, data access, breach notification, third-party cooperation, and customer remedies. Thus, effective protection

requires not only many regulations, but also coherence among those regulations (Sudirman et al., 2024).

Based on the above analysis, personal data protection in Indonesia has developed significantly but still faces several challenges in safeguarding customers effectively. Normatively, the existence of the Personal Data Protection Law, banking confidentiality rules, consumer protection regulations, and electronic transaction law shows that Indonesia already has a legal basis for customer protection. However, the effectiveness of these rules depends on law enforcement, institutional accountability, technological readiness, customer awareness, and legal culture. In practice, the protection of customer data will be weak if banks do not implement strong cybersecurity systems, if regulators do not supervise consistently, and if customers do not understand their rights. The banking sector must therefore treat personal data protection as a core element of risk management and consumer protection. Customer protection should not only be reactive after a data breach occurs, but also preventive through education, supervision, secure technology, and responsible governance. Therefore, the effectiveness of personal data protection in safeguarding customers requires continuous strengthening of regulation, enforcement, infrastructure, public awareness, and institutional responsibility.

Conclusion

Based on the discussion, it can be concluded that the protection of customer rights in Indonesia has obtained a relatively strong legal foundation through the Personal Data Protection Law, the Banking Law, consumer protection regulations issued by the Financial Services Authority, Bank Indonesia regulations, and the legal framework on electronic information and transactions. These regulations show that customer data protection is no longer limited to the principle of bank secrecy, but has developed into a broader protection of personal data, privacy rights, and consumer rights in the digital financial ecosystem. The existence of the Personal Data Protection Law is particularly important because it recognizes customers as data subjects who have rights over the collection,

processing, use, storage, and deletion of their personal data. However, the effectiveness of this protection does not depend solely on the availability of written rules, but also on the consistency of implementation by banks and the supervision carried out by relevant authorities. In practice, customer data remains vulnerable to misuse, unauthorized access, phishing, hacking, weak internal control, and data breaches in digital banking services. Therefore, the answer to the research problem is that Indonesian law has provided normative protection for customer rights, but its practical effectiveness still requires stronger enforcement, better institutional coordination, and more reliable technological safeguards. This means that customer data protection must be treated as a core element of banking governance, not merely as a formal administrative obligation.

Furthermore, the effectiveness of personal data protection in safeguarding customers is influenced by legal substance, law enforcement, facilities and infrastructure, public awareness, and legal culture. From the perspective of legal substance, Indonesia already has important regulations, but these rules must be supported by clearer technical standards and consistent application in banking practice. From the perspective of law enforcement, OJK, Bank Indonesia, and internal bank compliance units must strengthen supervision, complaint handling, sanction mechanisms, and accountability when data breaches occur. Banks must also improve cybersecurity infrastructure, employee training, risk management, authentication systems, and data breach response procedures to prevent harm to customers. At the same time, customers need better digital literacy so that they understand their rights, recognize potential risks, and know the legal steps available when their personal data is misused. Future research is recommended to examine the implementation of customer data protection in a wider range of banking institutions, including comparisons between conventional banks, digital banks, and financial technology platforms. Practically, banks and regulators should strengthen preventive protection, transparent notification mechanisms, effective compensation procedures, and a legal culture that recognizes personal data as an essential part of privacy, trust, and consumer justice.

E-ISSN: 3026-3182
Available online at website: https://journal.uib.ac.id/index.php/barjoules/index

References

Ahmad, F., Manurung, S. A., Silalahi, U., & Sudirman, L. (2025). The Urgency of Forming Legislation Regarding Online Loans in Indonesia: Legal Protection Solutions for the Community. *Jurnal Pembaharuan Hukum*, 12(1), 1–18. https://doi.org/10.26532/jph.v12i1.37895

Algamar, M. D., & Ismail, N. (2023). Data Subject Access Request: What Indonesia Can Learn adn Operationalise In 2024? *Journal of Central Banking Law and Institutions*, 2(3), 481–512. https://doi.org/10.21098/jcli.v2i3.171

Algamar, M. D., Munir, A. B., & Hendro, H. (2024). Managing Indonesian Data Breach Notification In The Financial Services Sector: A Case For One-Stop Notification Model. *Journal of Central Banking Law and Institutions*, 3(3), 547–584. https://doi.org/10.21098/jcli.v3i3.271

Alrawhani, E. M., Romli, A., & Al-Sharafi, M. A. (2025). Evaluating the role of protection motivation theory in information security policy compliance: Insights from the banking sector using PLS-SEM approach. *Journal of Open Innovation: Technology, Market, and Complexity*, 11(1), 100463. https://doi.org/10.1016/j.joitmc.2024.100463

Anbiya, Z. A. N., & Januarita, R. (2026). Tanggung Jawab Bank atas Investasi Ilegal Pegawai: Tinjauan UUPK dan GCG. B*andung Conference Series: Law Studies*, 6(1). https://doi.org/10.29313/bcsls.v6i1.21897

Annafa, S. W., Simanjuntak, H. P. G. H., & Ananda, A. M. (2024). Tanggung Jawab Hukum Bank dalam Kasus Kebocoran Data Nasabah. *Jurnal Multidisiplin Ilmu Akademik*, 1(6), 129–135. https://doi.org/10.61722/jmia.v1i6.2885

Antony, A., Sandoval, E. B., & Louis, J. E. (2025). Legal Reform in Indonesia's Response to the Digital Manipulation Era: A Responsive Legal Theory Approach. *Trunojoyo Law Review*, 8(1), 1–26. https://doi.org/10.21107/tlr.v8i1.30732

Antony, A., Sudirman, L., & Situmeang, A. (2026). Legal Research Methodology as a Critical Epistemological Framework for Legal Argumentation and Legal Development. *Barelang Journal of Legal Studies*, 4(1), 21–49. https://doi.org/10.37253/barjoules.v4i1.12379

Arbain, A., Fiancheto, D., Romadhon, R., & Sriadi, J. L. (2026). Personal Data Protection in the Banking Sector from the Perspective of Contextual Integrity: An Analysis on the Privacy Policies of State-Owned Banks. *Jurnal Indonesia Sosial Sains*, 7(4), 1269–1277. https://doi.org/10.59141/jiss.v7i4.2312

Ayunda, R., & Rusdianto, R. (2021). Perlindungan Data Nasabah Terkait Pemanfaatan Artificial Intelligence dalam Aktifitas Perbankan di Indonesia. *Jurnal Komunikasi Hukum*, 7(2), 663–677. https://doi.org/10.23887/jkh.v7i2.37995

Azza, A. A., & Taek, A. M. (2025). Batam City's Competitive Position as an Investment Destination in the Southeast Asia Region in 2021-2022. *Journal of World Trade Studies*, 9(2), 15–28. https://doi.org/10.22146/jwts.v9i2.18357

Bodhi, S., & Tan, D. (2022). Keamanan data pribadi dalam sistem pembayaran e-wallet terhadap ancaman penipuan dan pengelabuan (cybercrime). *UNES Law Review*, 4(3), 297–308. https://doi.org/10.31933/unesrev.v4i3.236

Cele, N. N., & Kwenda, S. (2025). Do cybersecurity threats and risks have an impact on the adoption of digital banking? *A systematic literature review. Journal of Financial Crime*, 32(1), 31–48. https://doi.org/10.1108/JFC-10-2023-0263

Chairunnisa, S., Murwadji, T., & Harrieti, N. (2024). Perlindungan Hukum Terhadap Nasabah atas Kejahatan Phising dan Hacking pada Layanan Bank Digital Ditinjau Berdasarkan Hukum Positif Indonesia. *HAKIM: Jurnal Ilmu Hukum dan Sosial*, 2(1), 1–16. https://doi.org/10.51903/hakim.v2i1.1535

Delpiero, M., Reynaldi, F. A., Ningdiah, I. U., & Muthmainnah, N. (2021). Analisis Yuridis Kebijakan Privasi dan Pertanggungjawaban Online Marketplace Dalam Perlindungan Data Pribadi Pengguna Pada Kasus Kebocoran Data. *Padjajaran Law Review*, 9(1), 1–22.

Disemadi, H. S. (2022). Lenses of Legal Research: A Descriptive Essay on Legal Research Methodologies. *Journal of Judicial Review*, 24(2), 289. https://doi.org/10.37253/jjr.v24i2.7280

Fikri, M., & Rusdiana, S. (2023). Ruang Lingkup Perlindungan Data Pribadi: Kajian Hukum Posistif Indonesia. *Ganesha Law Review*, 5(1), 39–57. https://doi.org/10.23887/glr.v5i1.2237

Irmawati, E., Pieries, J., & Widiarty, W. S. (2024). Perlindungan Hukum Atas Data Pribadi Nasabah Bank Pengguna Mobile Banking dalam Perspektif Uu No 27 Tahun 2022 tentang Kebocoran Data. *Jurnal Syntax Admiration*, 5(1), 12–27. https://doi.org/10.46799/jsa.v5i1.964

Johri, A., & Kumar, S. (2023). Exploring Customer Awareness towards Their Cyber Security in the Kingdom of Saudi Arabia: A Study in the Era of Banking Digital Transformation. *Human Behavior and Emerging Technologies*, 2023, 1–10. https://doi.org/10.1155/2023/2103442

Judijanto, L., Solapari, N., & Putra, I. (2024). An Analysis of the Gap Between Data Protection Regulations and Privacy Rights Implementation in Indonesia. *The Easta Journal Law and Human Rights*, 3(01), 20–29. https://doi.org/10.58812/eslhr.v3i01.351

Katiandagho, V., Putong, D. D., & Melo, I. J. (2023). Undang Undang Perlindungan Data Pribadi Memperkuat Undang Undang Perbankan dalam Menjaga Rahasia Data Nasabah & untuk Melindungi Data Pribadi Masyarakat Indonesia. *Jurnal Hukum to - ra*, 9(1), 106–114. https://doi.org/10.55809/tora.v9i1.212

Kurniawan, D. A., Aliyah, R., & Rizqi, A. M. (2024). Tanggung Jawab Hukum Bank Digital terhadap Perlindungan Konsumen di Indonesia. *JATIJAJAR LAW REVIEW*, 3(2), 81. https://doi.org/10.26753/jlr.v3i2.1584

Kurniawan, K. D., Hehanussa, D. J. A., Setiawan, R., Susilowati, I., Sopian, S., & Helfisar, D. (2024). Criminal Sanctions and Personal Data Protection in Indonesia. *Lex Publica*, 11(2), 221–247. https://doi.org/10.58829/lp.11.2.2024.255

Manurung, S. A., Irawati, J., Sudirman, L., Agustianto, A., & Farahdina, F. (2025). Comparison of Agreement Law in Indonesia and Malaysia: Phenomenon of Standard Agreement Practices. *SASI*, 31(1), 60–69. https://doi.org/10.47268/sasi.v31i1.2683

Munawaroh, S., Mufidah, N. Z., Haryadi, W. T., & Tilman, A. M. (2025). The Urgency of Civil Code Reform That Is Responsive to the Needs of Modern Digital Business. *Rechtidee*, 20(2), 166–185. https://doi.org/10.21107/ri.v20i2.31551

Nagari, S. F., & Raharja, S. (2025). Cyber Security Awareness, Knowledge and Behavior of Digital Banking Users in Salatiga. *Asia Pacific Fraud Journal*, 10(1), 15–29. https://doi.org/10.21532/apfjournal.v10i1.398

Nasution, A. H. (2025). The Urgency of Customer Personal Data Protection in Digital Banking. *Rechtsvinding*, 3(1), 153–162. https://doi.org/10.59525/rechtsvinding.v3i1.814

Nurkholisah, S., Rismana, D., Nugroho, A. E., Munjiyah, A., & Ayunisa, Q. (2025). Deepfake Sebagai Bentuk Kejahatan Siber Baru: Tantangan Kriminalisasi Dalam Hukum Pidana Indonesia. *JURNAL USM LAW REVIEW*, 8(3), 2421–2445. https://doi.org/10.26623/julr.v8i3.13060

Purnama, T. D., & Alhakim, A. (2021). Pentingnya UU Perlindungan Data Pribadi sebagai Bentuk Perlindungan Hukum terhadap Privasi di Indonesia. *Jurnal Komunitas Yustisa,* 4(3), 1056–1064.

Putri, B. M. L., Rohaini, R., Nhung, P. H., & Putri, R. W. (2025). Analysis of Consumer Rights Protection Against the Misuse of Personal Data in Fintech Services. *Lex Publica*, 12(1), 32–62. https://doi.org/10.58829/lp.12.1.2025.286

Putri, D. D. F., & Fahrozi, M. H. (2021). Upaya Pencegahan Kebocoran Data Konsumen Melalui Pengesahan RUU Perlindungan Data Pribadi (Studi Kasus E-Commerce Bhinneka.Com). *Borneo Law Review*, 5(1), 46–68. https://doi.org/10.35334/bolrev.v5i1.2014

Putri, D. F., Andriani, A., Sari, W. R., & Nabbila, F. L. (2023). Analisis Perlindungan Nasabah Bsi Terhadap Kebocoran Data Dalam Menggunakan Digital Banking. *Jurnal Ilmiah Ekonomi dan Manajemen*, 1(4), 173–181. https://doi.org/10.61722/jiem.v1i4.331

Rahmawati, I. N., Ramadani, N., Heni, D. R., & Kevin, S. (2023). Pertanggung jawaban Pihak Bank terhadap Kebocoran Data Diri Nasabah. *AUFKLARUNG : Jurnal Pendidikan, Sosial dan Humaniora*, 3(2), 208–215.

Rosadi, S. D., Noviandika, A., Walters, R., & Aisy, F. R. (2023). Indonesia's personal data protection bill, 2020: does it meet the needs of the new digital economy? *International Review of Law, Computers & Technology*, 37(1), 78–90. https://doi.org/10.1080/13600869.2022.2114660

Rumbruren, A., & Watofa, Y. (2025). Analysis of the Responsibilities of the Organizer of the Electronic System in Case of Data Breach. *Awang Long Law Review,* 7(2), 481–491. https://doi.org/10.56301/awl.v7i2.1549

Setiawan, H. B., & Najicha, F. U. (2022). Perlindungan Data Pribadi Warga Negara Indonesia Terkait Dengan Kebocoran Data. *Jurnal Kewarganegaraan*, 6(1), 976–982. https://doi.org/10.31316/jk.v6i1.2657

Shahrullah, R. S., Park, J., & Irwansyah, I. (2024). Examining Personal Data Protection Law of Indonesia and South Korea: The Privacy Rights Fulfilment. *Hasanuddin Law Review*, 10(1), 1–20. https://doi.org/10.20956/halrev.v10i1.5016

Silviani, N. Z., Shahrullah, R. S., Atmaja, V. R., & Hyun, P. J. (2023). Personal Data Protection in Private Sector Electronic Systems for Businesses: Indonesia vs. South Korea. *Jurnal Hukum dan Peradilan*, 12(3), 517. https://doi.org/10.25216/jhp.12.3.2023.517-546

Sriono, S., Risdalina, R., Kusno, K., M, I. K., & Syahyunan, H. (2024). Legal Protection for Digital Bank Customers in Indonesia: Analysis of Data Confidentiality Regulations and Bank Responsibility. *LITIGASI*, 25(2), 301–330. https://doi.org/10.23969/litigasi.v25i2.18538

Sudirman, L., Disemadi, H. S., & Jerryen, J. (2024). Bentuk Pengaturan Perbankan Digital di Negara Indonesia dan Singapura. *Legal Spirit*, 8(2), 325–340. https://doi.org/10.31328/ls.v8i2.5438

Sulistyandari, S., & Sutrisno, P. A. (2023). Legal Aspects and Role of Ojk In Bank Digital by Digital Banking Services During Post-Covid 19 Pandemic in Indonesia. *Journal of Law and Sustainable Development*, 11(12), e2364. https://doi.org/10.55908/sdgs.v11i12.2364

Tan, D. (2021). Metode Penelitian Hukum: Mengupas Dan Mengulas Metodologi Dalam Menyelenggarakan Penelitian Hukum. *Nusantara: Jurnal Ilmu Pengetahuan Sosial*, 8(8), 2463–2478. http://jurnal.um-tapsel.ac.id/index.php/nusantara/article/view/5601/3191

Waliullah, M., George, M. Z. H., Hasan, M. T., Alam, M. K., Munira, M. S. K., & Siddiqui, N. A. (2025). Assessing the Influence of Cybersecurity Threats and Risks on the Adoption and Growth of Digital Banking: A Systematic Literature Review. *American Journal of Advanced Technology and Engineering Solutions*, 01(01), 226–257. https://doi.org/10.63125/fh49az18

Wang, S., Asif, M., Shahzad, M. F., & Ashfaq, M. (2024). Data privacy and cybersecurity challenges in the digital transformation of the banking sector. *Computers & Security*, 147, 104051. https://doi.org/10.1016/j.cose.2024.104051

Weley, N. C., & Disemadi, H. S. (2022). Implikasi Hukum Pemasangan CCTV di Tempat Umum secara Tersembunyi terhadap Perlindungan Data Pribadi. *Amnesti : Jurnal Hukum*, 4(2), 79–93. https://doi.org/10.37729/amnesti.v4i2.2151

Wibowo, A., Alawiyah, W., & Azriadi. (2024). The importance of personal data protection in Indonesia's economic development. *Cogent Social Sciences*, 10(1), 2306751. https://doi.org/10.1080/23311886.2024.2306751

Widiatedja, I. G. N. P., & Mishra, N. (2023). Establishing an independent data protection authority in Indonesia: a future–forward perspective. *International Review of Law, Computers & Technology*, 37(3), 252–273. https://doi.org/10.1080/13600869.2022.2155793

Widjaja, G. (2026). The Legal Implications of Personal Data Protection For Electronic Contracts From The Perspective of Indonesia Civil Law. *International Journal of Social and Education (INJOSEDU)*, 3(1), 125–138. https://doi.org/10.5281/zenodo.19533508

Yuspin, W., Putri, A. O., Fauzie, A., & Pitaksantayothin, J. (2024). Digital Banking Security: Internet Phishing Attacks, Analysis and Prevention of Fraudulent Activities. *International Journal of Safety and Security Engineering*, 14(6), 1699–1706. https://doi.org/10.18280/ijsse.140605

Yuspin, W., Wardiono, K., Nurrahman, A., & Budiono, A. (2023). Personal Data Protection Law in Digital Banking Governance in Indonesia. *Studia Iuridica Lublinensia*, 32(1), 99–130. https://doi.org/10.17951/sil.2023.32.1.99-130

Acknowledgments

None.

Competing Interest

The authors declare that there are no competing interests.