International Journal of Multicultural and Multireligious Understanding

http://ijmmu.com
editor@ijmmu.com
ISSN 2364-5369
Volume 12, Issue 6
June, 2025
Pages: 293-301

The Analysis of Bank's Responsibility for Customer Losses in Cases of Personal Data Misuse

Dea; Aisy Cantika; Ade Kevin Dwi Candra Putra; Farahdinny Siswajanthy; Lindryani Sjofjan

Department of Law, Pakuan University, Bogor, Indonesia

http://dx.doi.org/10.18415/ijmmu.v12i6.6888

Abstract

This study aims to analyze the responsibility of banks in managing customer personal data and how banks can protect such data from misuse threats. As financial institutions, banks have a significant responsibility to safeguard the confidentiality and security of customer data. This responsibility includes the use of encryption systems, strict internal policies, and transparency in data management. The misuse of personal data, both by external and internal parties, can result in losses for customers, who are entitled to compensation. Existing regulations provide legal protection for customers, and banks are required to follow established procedures in handling personal data misuse cases. This study also provides recommendations to strengthen security systems, transparency, and claims procedures within banking.

Keywords: *Bank Responsibility; Personal Data; Data Misuse; Data Protection Regulations; Data Security*

Introduction

Banking in Indonesia has grown rapidly along with the development of digital technology. Banks now offer various services through digital platforms that make it easier for customers to make transactions, such as internet banking and mobile banking. This transformation provides greater convenience, efficiency, and accessibility for the public. However, this progress also brings major challenges, especially in terms of protecting customers' personal data. Increasingly sophisticated digital services open up opportunities for cybercrime threats that risk leaking customers' personal data that should be protected by banks (Kurniawan & Hapsari, 2021). Customers' personal data, such as account information, transactions, and personal identities, are often the main targets for cybercriminals. In some cases, this data leak not only causes financial losses for customers, but also reputational losses that can threaten public trust in the banking system (Jacqueline et al., 2025).

The security of customers' personal data is a very important issue, considering the large amount of sensitive data managed by banks, both offline and online. This misuse of personal data can occur through various methods, such as hacking, illegal access to information, or carelessness on the part of internal bank parties who do not maintain the confidentiality of customer data. These incidents create a detrimental impact on customers, both in the form of material and non-material losses. Therefore, the

bank's responsibility to maintain the security and confidentiality of customer personal data must be taken seriously and made a top priority in digital banking operations (Akbar et al., 2024). Banks must have clear policies and procedures regarding personal data protection and ensure that the systems used are safe from the threat of cybercrime that continues to grow.

These cases of misuse of personal data require further evaluation of how banks are legally responsible for protecting customer data. Based on Law No. 8 of 1999 concerning Consumer Protection and Law No. 11 of 2008 concerning Information and Electronic Transactions (ITE), banks are required to protect customer personal data with high and accountable security standards (Taurus et al., 2023). However, in reality, there are still many cases of data misuse that cause losses to customers, which shows that the protection of personal data implemented by banks is not fully effective. Therefore, it is important to conduct a study on how much responsibility the bank has in cases of misuse of personal data and the protection mechanisms that must be implemented by the bank so that similar incidents do not happen again in the future. The purpose of this study is to analyze the extent of the bank's responsibility in protecting customer personal data, especially in cases of data misuse that cause losses to customers. This study also aims to identify efforts that can be made by banks to prevent misuse of personal data and the legal protection that exists for customers who are harmed by data leaks. Through this study, it is hoped that a deeper understanding can be obtained regarding the responsibility of banks and the preventive measures that must be implemented in protecting customer data so that losses caused by data misuse can be minimized.

Literatur Review

Understanding Bank Responsibility

Bank responsibility is an obligation that banks have to carry out their operations and services to customers with the principles of prudence, transparency, and protecting customer interests. This responsibility is not only limited to providing efficient financial services in accordance with applicable regulations, but also to protecting customers' personal data. Personal data, which includes personal information, transactions, and customer financial data, must be managed in a safe and responsible manner by the bank, considering the sensitivity of the information. In addition, banks are also required to maintain the confidentiality and security of customer data, which includes preventing data leaks that can be exploited by unauthorized parties. This responsibility, as stipulated in various banking regulations, includes the obligation to maintain the integrity and confidentiality of data received and processed by the bank (Widya et al., 2025). In general, banks are expected to play an active role in maintaining public trust by implementing an appropriate data protection system that is responsive to possible threats.

In addition to data protection, banks must also ensure that all policies and actions taken in protecting customer data are in accordance with the principles of prudence regulated by national and international regulations. Banks that fail to fulfill this obligation may face lawsuits from customers, which could potentially damage the reputation and integrity of the banking institution. Therefore, in addition to strengthening internal policies, banks must also pay attention to compliance with existing regulations and maintain clear communication with customers regarding the data protection measures implemented (Hendarto, 2024).

Misuse of Personal Data in Banking

Misuse of personal data in the banking context occurs when information that should be protected by the bank falls into the hands of unauthorized parties and is used for purposes that harm customers. Cases of misuse of personal data in the banking world include various forms of crime, such as identity theft, illegal access to accounts, and financial fraud through leaked information. This data misuse can be

carried out by internal parties, such as irresponsible bank employees, or external parties, such as hackers who break into the bank system to illegally obtain customers' personal data (Efendi et al., 2024).

Along with the increasing digitalization in the banking sector, cybercrimes related to misuse of personal data are becoming more frequent. Various hacking techniques, such as phishing, malware, and other techniques, are used by irresponsible parties to access customer data illegally. This crime not only threatens the financial security of customers but also threatens their privacy. Digital banking that relies on electronic transactions and data storage in digital form is an easy target for cybercrime. Therefore, banks are required to implement an integrated security system and use the latest technology to reduce the risk of customer personal data leakage.

Types of Personal Data Misuse

1. Identity Theft: Identity theft is the most common form of personal data misuse in banking. In this case, a customer's personal information, such as an account number or credit card number, is used by an irresponsible party to gain unauthorized access to the customer's account and make detrimental transactions. According to the OJK report, the number of identity theft cases in the digital banking sector has increased rapidly in recent years (OJK, 2020).
2. Illegal Access to Accounts: Misuse of personal data can also occur in the form of illegal access to a customer's account. In this case, leaked data, such as a password or PIN, is used to transfer or withdraw funds without the customer's permission. This type of incident often occurs through system hacking or other security breaches that leak sensitive information.
3. Electronic Fraud (Phishing): In this type of data misuse, an irresponsible party tries to deceive customers and banks by posing as an authorized party. They send emails, text messages, or phone calls asking customers to provide personal information such as passwords or credit card numbers for unclear reasons. This phishing technique is often used to gain unauthorized access to customer accounts.

Regulations and Legal Protection in Banking

As an institution that manages customers' personal data, banks are required to comply with various existing regulations, both at the national and international levels. In Indonesia, there are a number of regulations that govern the protection of customers' personal data. Law No. 8 of 1999 concerning Consumer Protection gives consumers the right to obtain protection for personal data and information held by institutions, including banks. In addition, Law No. 11 of 2008 concerning Information and Electronic Transactions (ITE) also regulates the security of personal data transmitted through electronic channels, and stipulates sanctions for parties who violate the privacy rights and security of customer data (Putri et al., 2024).

In addition to these regulations, Bank Indonesia and the Financial Services Authority (OJK) also have regulations related to customer data protection, which include the arrangement of security systems that must be implemented by banks. OJK has issued various guidelines that require banks to have a security system that meets international standards, including the use of encryption to protect customer data that is stored and processed. Banks are also required to provide a clear mechanism for customers to report incidents of misuse of personal data and provide compensation or restitution if customers suffer losses due to data leaks (Hendarto, 2024).

Personal Data Protection Regulations

Banks are required to comply with the provisions set by Bank Indonesia and OJK in securing customer data. One of the main rules is the obligation of banks to implement encryption and a two-factor authentication system in digital transactions to prevent unauthorized access to customer accounts. In

addition, banks must conduct regular training for employees and ensure that applicable data protection procedures are well understood by all parties involved in managing customer data (Hendarto, 2024). In addition, customers must also be given clear information regarding bank policies regarding the management and protection of their personal data.

Research Method

1. Type of Research

This study uses a literature study method, which is a non-experimental research approach that aims to analyze and evaluate various existing references related to bank responsibility for misuse of customer personal data. This literature study investigates relevant written sources, including laws, banking regulations, personal data protection policies, and scientific articles that discuss the obligations and regulations implemented by banks in protecting customer data.

2. Data Sources

This study relies on various types of data sources to enrich the analysis and understand more deeply the topic being studied. The data sources used in this study include:

- Books, scientific journals, and legal articles related to banking and personal data protection. These sources provide a theoretical basis and academic perspective that leads to an understanding of the role of banks in protecting customer personal data and how this policy is implemented in practice.
- Legislation governing personal data protection, including Law No. 8 of 1999 concerning Consumer Protection and Law No. 11 of 2008 concerning Information and Electronic Transactions (ITE). This regulation is the legal basis that requires banks to maintain the confidentiality of customer data and be responsible for misuse of such data.
- Documents and regulations from the Financial Services Authority (OJK) and Bank Indonesia regarding the management and protection of personal data. OJK and Bank Indonesia as regulators of the banking sector in Indonesia issue guidelines and regulations that must be adhered to by banks in protecting customer data and preventing misuse of personal information.

3. Research Focus

This research focuses on two main areas:

- Legal Research: The main focus of this research is to examine the legal regulations governing banks' obligations to protect customers' personal data. This includes an analysis of the bank's legal responsibilities in the event of data misuse, as well as the regulations that banks must comply with to protect customer data from potential leaks or misuse by third parties. This legal research aims to understand more clearly how the law provides protection to customers and ensures that banks act in accordance with applicable provisions.
- Case Studies: This research will also analyze case studies related to the misuse of customers' personal data in the banking sector. These cases may include incidents involving hacking of bank systems resulting in data leaks, as well as negligence by internal bank personnel resulting in customer data falling into the wrong hands. Analyzing real cases will provide an understanding of the challenges faced by banks in managing and protecting customer data and how banks respond to such incidents.

4. Analysis Method

This study will use descriptive analysis to describe and assess the existing findings from the literature that has been analyzed. Some aspects that will be analyzed include:

- Data Protection Regulations and Policies: The author will describe various relevant laws and regulations related to the protection of customer personal data, including provisions set by the OJK and Bank Indonesia. This study will analyze the extent to which these regulations are implemented in banking practice.

- Bank Policies in Data Protection: The author will describe the steps taken by banks in managing and protecting customer data, both in terms of cybersecurity, the use of encryption technology, and internal procedures to handle potential data leaks.

- Bank Solutions and Responsibilities: This analysis will also assess the solutions provided by banks when there is misuse of customer personal data. This includes compensation or restitution policies for customers who are harmed, as well as reporting and dispute resolution mechanisms that can be accessed by customers. The author will evaluate the extent to which these policies provide a sense of security for customers and reduce the impact of losses due to data misuse.

Using a descriptive analysis method, this study aims to provide a clear picture of the implementation of data protection regulations and policies by banks and assess their effectiveness in protecting customer personal data and providing fair solutions for customers who are harmed.

Result

Bank Responsibilities in Managing Customer Personal Data

Banks, as financial institutions operating in the digital world, have a great responsibility in protecting customer personal data. Customer personal data, which includes sensitive information such as account numbers, transactions, personal identities, and other financial data, is very vulnerable to misuse if not managed properly. The bank's responsibilities in this case include several important aspects, namely:

1. Personal Data Security

One of the main obligations of the bank is to ensure that customer personal data is protected from all forms of external and internal threats. Banks must implement a comprehensive security system to prevent unauthorized access to customer data. One of the main ways to ensure data security is to use an encryption system that can secure data stored in the bank's electronic system. This encryption functions to convert sensitive data into a format that can only be read by authorized parties even if the data is successfully accessed by unauthorized parties. Encryption is one of the most effective steps in protecting sensitive data from cyber threats. In addition, regular security system updates must be carried out to anticipate potential threats from hackers or data leaks that are increasingly sophisticated along with the development of information technology (Ningsih & Ismaini, 2025).

2. Internal Data Management Policy

Banks are required to have strict internal policies in managing customer data. This policy includes regulating data access that is limited to authorized and trusted parties only, as well as implementing a two-factor authentication system to access customer data. The implementation of two-factor authentication is important to increase the level of data security, especially in digital transactions

involving customer personal information. Banks are also required to have clear procedures regarding the handling of personal data in various situations, including when data leaks occur. The existence of this internal policy is very important to prevent misuse of data by internal and external parties that can harm customers (Tamiwaluya et al., 2024).

3. Transparency in Data Management

Banks are also required to provide full transparency to customers regarding how their data is used and protected. According to the Consumer Protection Law No. 8 of 1999, banks must provide clear information regarding the purpose of data collection, the parties who can access the data, and how the data will be used. This information must be conveyed transparently to customers, either through a service agreement or a privacy policy that is easy for customers to understand. By providing clear information, banks not only comply with applicable regulations, but also strengthen customer trust in the data protection system implemented.

Misuse of Customer Personal Data

Misuse of customer personal data in the banking sector is an increasing problem, both due to hacking by external parties and negligence by internal parties of the bank. In many cases, banks are often the ones blamed for being negligent in maintaining the security of customer data. This misuse of personal data can be caused by several factors, namely:

1. Misuse of Data by External Parties (Hacking)

Data misuse is often carried out by hackers who have managed to gain illegal access to the bank system. They can steal sensitive information such as account numbers, PINs, and customer credit card information, which are then used to commit financial fraud or other illegal transactions (Tamiwaluya et al., 2024). In cases of hacking, customer personal data is often used to withdraw funds without the account owner's knowledge. This cybercrime shows how vulnerable customer personal data is if the bank does not have an adequate security system. Data leaks that occur through online transactions or unsafe banking applications have a very detrimental impact on customers, both in the form of financial losses and loss of privacy.

2. Negligence of Internal Bank Parties

In addition to threats from external parties, negligence committed by internal bank parties, such as employees who do not maintain the confidentiality of customer data, can also be a cause of misuse of personal data. For example, employees who intentionally or unintentionally access customer data without permission or do not follow applicable data security procedures (Ningsih & Ismaini, 2025). This case often raises questions about the bank's responsibility in maintaining internal integrity and supervising employee activities in managing customer personal data. This internal negligence can also be caused by a lack of training for employees regarding the handling of personal data and information security.

Bank Responsibilities in Cases of Misuse

In the event of misuse of personal data, the injured customer has the right to claim compensation for the losses they have suffered. For example, if there is a theft of funds due to a data leak, the customer can file a claim with the bank to obtain compensation for the financial losses incurred. As a financial institution, banks must ensure that they have a clear and effective claims handling mechanism to protect customers from losses due to misuse of personal data. This process includes prompt investigation, compensation, and steps to prevent similar incidents from happening again in the future.

Banks are also required to conduct regular internal audits to ensure that data security policies are running well and to assess the potential risk of data leaks. If there is a failure to maintain the security of customer data, the bank can be subject to sanctions in accordance with applicable regulations and be responsible for the losses experienced by the customer (Sudirman et al., 2024).

Legal Protection for Customers

In Indonesia, existing regulations provide legal protection for customers who are victims of misuse of personal data. Some relevant regulations in this regard include:

1. Personal Data Protection Regulation Law No. 11 of 2008 concerning Information and Electronic Transactions (ITE) provides a legal basis for the protection of personal data in electronic transactions. In the ITE Law, banks are required to maintain the confidentiality of customers' personal data and are responsible if data leaks occur. In addition, the Financial Services Authority (OJK) and Bank Indonesia also issue guidelines and regulations governing banks' obligations to maintain the confidentiality and security of customer data, as well as dispute resolution mechanisms in the event of a data leak.

2. Customer Rights to Obtain Compensation Customers who are victims of personal data misuse have the right to receive compensation for the losses they experience, both in the form of financial losses and non-financial losses, such as loss of reputation or privacy. Banks are required to follow the procedures set by the OJK or related agencies in handling cases of personal data misuse. This step includes an internal investigation into the misuse that occurs and providing compensation in accordance with the losses experienced by the customer. In some more serious cases, customers can also report this incident to the National Commission for Personal Data Protection (KNPD) or the relevant consumer protection agency.

3. Preventive Measures and Policy Updates To reduce the risk of future data leaks, banks must continue to update their existing security policies and data protection systems. More sophisticated encryption technology, the implementation of strict security protocols, and regular training for employees on the importance of personal data protection are some of the preventive measures that banks can take. These measures are not only to reduce the risk of personal data leaks, but also to strengthen customer trust in the banking system.

By strengthening data protection and guaranteeing customers' rights to the confidentiality of their personal information, banks can maintain their reputation and credibility in the eyes of the public and ensure that they fulfill their established legal responsibilities.

Conclusion

This study reveals that the responsibility of banks in managing customer personal data is very large, considering that the data held by banks is very sensitive information. Banks are required to ensure that customer personal data is protected with an adequate security system, through the use of encryption systems, regular security system updates, and strict internal policies regarding data management. Transparency in managing personal data is also very important to maintain customer trust in the bank.

Misuse of customer personal data often occurs either due to hacking by external parties or internal negligence of the bank. Banks are often questioned about their responsibility if a data leak occurs that results in losses for customers. In this case, customers are entitled to compensation for losses arising from the misuse of their personal data. Existing regulations, such as the Consumer Protection Act and the ITE Act, provide legal protection for customers who are victims of misuse of personal data, and ensure

that banks are responsible for data leaks that occur. With the increasing threat to personal data, banks must continue to update their security policies and systems in order to reduce the risk of customer personal data leaks in the future. Therefore, it is important for banks to strengthen their efforts to protect personal data by using the latest technology, and ensuring that all internal parties follow applicable security procedures.

Recommendations

1. Banks must continue to update and improve existing security systems, including using more sophisticated encryption technology and stricter security protocols to anticipate increasingly complex hacking threats.

2. Banks need to provide regular training to all employees regarding the management of customer personal data and the procedures that must be followed to maintain data confidentiality.

3. Banks must provide more transparent information to customers regarding the use and management of their personal data, as well as the protection measures implemented by the bank to reduce customer concerns about data misuse.

4. Banks must strengthen the mechanism for handling claims and providing compensation for customers who are victims of personal data misuse. These procedures must be clear and easily accessible to customers.

Refrences

Akbar, R., Irwan, M., & Nasution, P. (2024). Analisis Keamanan Data Pada Aplikasi Mobile Banking Journal of Sharia Economics Scholar (JoSES). *Journal of Sharia Economics Scholar (JoSES)*, *2*(2), 79–83.

Efendi, T. K., Esza, M., Firmanda, M., Alfarisy, F. R., Javantara, A. C., & Indrarini, R. (2024). *Analisis Kebijakan Perlindungan Nasabah Pada Bank Digital Syariah di Indonesia*. *2*(November), 1–7.

Hendarto, I. S. (2024). *IMPLIKASI PENGARUH MINIMNYA PENGATURAN PERLINDUNGAN PRIVASI DATA PRIBADI NASABAH PADA PERBANKAN DIGITAL*. *04*(02), 129–140.

Jacqueline, A., Gunardi, S., Moody, L., & Syailendra, R. (2025). *Perlindungan Kepada Nasabah Bank Terhadap Kebocoran Data (Studi Kasus Kebocoran Data pada Bank Indonesia)*. *2*(1), 107–114.

Kurniawan, K. D., & Hapsari, D. R. I. (2021). Kejahatan Dunia Maya Pada Sektor Perbankan Di Indonesia: Analisa Perlindungan Hukum Terhadap Nasabah. *Pleno Jure*, *10*(2), 122–133. https://doi.org/10.37541/plenojure.v10i2.590.

Ningsih, A. S., & Ismaini, D. (2025). *Keamanan data nasabah bank syariah*. *2*(1), 651–662.

OJK. (2020). *Laporan tahunan OJK: Statistik kejahatan siber di sektor perbankan. OJK.*

Putri, S. N. M., Putra, M. M., Azzam, M. F., & Andika, A. P. (2024). Implikasi Regulasi Perbankan Terhadap Keamanan Data Nasabah: Tinjauan Terhadap Perlindungan Data Nasabah. *Jurnal Multidisiplin …*, *8*(6), 327–337. https://sejurnal.com/1/index.php/jmi/article/view/2379%0Ahttps://sejurnal.com/1/index.php/jmi/article/download/2379/2766.

Sudirman, L., Disemadi, & Jerryen. (2024). *Bentuk Pengaturan Perbankan Digital di Negara Indonesia dan Singapura*. *8*(2), 325–340.

Tamiwaluya, M. G. P., Rokhim, A., & Anadi, Y. R. (2024). *PERLINDUNGAN HUKUM PENYALAHGUNAAN DATA PRIBADI NASABAH SEBAGAI KONSUMEN PERBANKAN BERKAITAN DENGAN RAHASIA BANK (Studi Kasus di PT Bank Muamalat KC Surabaya)*. 10339–10349.

Taurus, K. S., Dewanto, W., & Anggawira. (2023). PERLINDUNGAN HUKUM BAGI NASABAH DALAM PENGGUNAAN DATA PRIBADI OLEH BANK UNTUK TUJUAN KOMERSIL KEPADA PIHAK KETIGA. *Jurnal Ilmiah Indonesia*, *8*(10), 5744–5760.

Widya, D., Simatangkir, E., Semarang, U. N., Semarang, U. N., Faliha, N. S., & Semarang, U. N. (2025). *KEAMANAN SIBER DALAM PERBANKAN SERTA TANTANGAN*. *2*(1), 33–42.

Copyrights