International Journal of Social Welfare and Family Law

E-ISSN: 3047-7727
P-ISSN: 3047-4841

Research Article

Legal Protection For Customers Resulting From Personal Data Leaks In Credit Agreements At PT Bpr Karya Sari Sedana

Dwi Nova Indriyani [1*], Johannes Ibrahim Kosasih [2], and Ni Komang Arini Styawati [3]

[1] Universitas Warmadewa, Indonesia; e-mail : dwinovaindriyaniii@gmail.com
[2] Universitas Warmadewa, Indonesia; e-mail : johonesibrahim26@gmail.com
[3] Universitas Warmadewa, Indonesia; e-mail : komangarini25@gmail.com
* Corresponding Author : Dwi Nova Indriyani

Abstract: The economy of a country, including Indonesia, is a system that encompasses all production, distribution, and consumption activities occurring within the country. In the economy, problems often arise that can affect the welfare of society. The problem formulation in this study is: How is the regulation and supervision of both internal and external banks carried out to prevent customer personal data leakage in credit agreements? And how is the responsibility of BPR Karya Sari Sedana towards the leakage of customer debtor data? The research method used is empirical legal research. The conclusion in the study is the protection of customer data against personal data leakage by understanding the forms of supervision from both internal and external parties conducted by the banking institution and referring to the OJK regulations that have been established, in order to minimize the recurrence of similar incidents and allow the public to conduct transactions safely without worrying about their personal data. Leaked by irresponsible individuals. The responsibility carried out by the banking sector currently, namely the Financial Services Authority Regulation Number 22 of 2023 concerning Consumer and Community Protection in the Financial Services Sector, also regulates consumer protection in the financial services industry. Forms in policies related to regulations in the banking world ensure that the public does not worry about their personal data.

Keywords: Accountability; Banking; Consumer Protection; Data Leaks; Economy.

Received: January 05, 2026
Revised: February 10, 2026
Accepted: March 09, 2026
Published: April 08, 2026
Curr. Ver.: April 08, 2026

1. Introduction

The banking industry in Indonesia has become increasingly important, highlighting the essential role of banking institutions in the economy. This sector serves a strategic function in supporting national development, particularly in achieving more balanced and equitable growth. A well-developed banking industry is often associated with stronger economic stability and progress within a country. Consequently, the performance of banks is commonly evaluated based on their financial outcomes.

As a major component of the financial system, banking institutions act as key drivers of economic activity and are closely linked to national development efforts. Broadly speaking, banking law encompasses the regulations that govern all aspects of banking, including institutional frameworks, business operations, and procedural practices. The primary role of

banks is to mobilize funds from the public and redistribute them to support economic activities. Furthermore, banks play a vital role I stimulating economic growth, and the advancement of the banking sector is frequently used as a benchmark for assessing a country's overall economic performance.

Advances in information technology and the digitalization of banking services have provided convenience and efficiency in managing customer data, including at Rural Credit Banks (BPR). Digitization enables banks to perform various operational activities, from account opening and transaction monitoring to credit disbursement, more quickly and accurately. However, this progress also poses a new risk: the leakage of customer personal data. Customer data is a critical asset for banks because it contains sensitive information, such as identity, account details, transaction history, and other financial information (Nurdin, 2018). Misuse of this data can result in financial losses for customers, damage the bank's reputation, and undermine public trust in the banking system as a whole.

Data leaks at rural banks (BPR) can occur due to various factors, both internal and external. Internal factors include employee negligence, weak internal oversight, or unethical practices such as the sale of customer data by marketing agencies. External factors include cyberattacks, hacking, or fraud by irresponsible third parties. Data leak cases demonstrate that even though banks have implemented security systems, risks remain and can have far-reaching impacts on both customers and the bank itself. Incidents like these highlight the urgency of legal protection and stricter oversight mechanisms in the banking sector.

As a financial institution, Rural Banks (BPRs) have a legal responsibility to maintain the confidentiality and security of customer data. This is in line with the Personal Data Protection Law (PDP Law) Number 27 of 2022, which stipulates that every personal data manager is obliged to protect the rights of data subjects and implement the principles of security, transparency, and accountability in data processing. Furthermore, the Financial Services Authority (OJK) regulates and supervises the banking sector through POJK Number 22 of 2023 concerning Consumer and Public Protection in the Financial Services Sector (Tarigan & Paulus, 2019). This POJK emphasizes the need for customer data protection, the application of prudential principles in data management, and a complaint resolution mechanism in the event of data leaks or misuse.

In practice, data breaches at rural banks (BPRs) often arise from poorly controlled internal activities, such as marketing processes involving the exchange or sale of customer data between marketing staff. This practice, known as "call connection," is carried out to facilitate the marketing of banking products such as unsecured loans or credit cards. While this practice is considered beneficial internally, it violates the principle of personal data protection and poses legal risks for the bank. Furthermore, misuse of customer data can occur through unauthorized access by third parties, either through digital systems or manual administrative mechanisms, which can cause financial and psychological harm to customers.

In the context of banking law, the relationship between a bank and its customers is not simply a contractual one. Banks are obligated to maintain customer confidentiality and process data in accordance with legal provisions. Legal protection for customers is twofold: preventive and repressive . Preventive protection aims to prevent data leaks, for example through digital security procedures, employee training, and internal audits. Repressive

protection is implemented through law enforcement after a violation occurs, including administrative, civil, and criminal sanctions against parties who are negligent or misuse data.

The PDP Law affirms the data subject's right to access, correct, or delete misused data. This is crucial, especially if the leaked data impacts a customer's reputation or credit standing in banking systems, such as BI Checking. Through this mechanism, customers have a legal basis to seek compensation and restore their rights. Furthermore, the Financial Services Authority (POJK) and other relevant regulations emphasize banks' responsibility to implement adequate security systems for electronic transactions, personal data management, and protection from cybercrime risks.

The data breach at the rural bank (BPR) underscores the need to internalize a data security culture across all levels of bank staff. Banks must implement prudent principles from account opening and identity verification to credit disbursement, ensuring that customer data is accurate and valid. Banks must also prepare emergency response procedures in the event of a breach, including notification to affected customers and corrective measures to prevent similar incidents in the future. In this way, banks not only fulfill their legal obligations but also build customer trust in the banking industry in general Ginara et al., 2022).

Legal protection of customer personal data in rural banks (BPR) is part of efforts to safeguard human rights, public trust, and the stability of the national financial system. This study is crucial to understanding how internal and external regulatory and oversight mechanisms work to prevent data breaches, and to what extent existing regulations and practices are able to protect customers from the risks arising from the digitalization of banking services.

Based on this description, it is important to examine the legal protection provided to customers for personal data leaks in credit agreements, as well as the bank's responsibilities in the event of a customer data leak. Therefore, this study aims to analyze the legal protection provided to customers and the responsibilities of PT BPR Karya Sari Sedana in maintaining the security of customers' personal data in credit agreements.

2. Proposed Method

In this section, you need to describe the proposed method step by step. Explanations This study uses an empirical legal research type that aims to examine the application of legal protection for customers regarding personal data leaks in credit agreements at PT BPR Karya Sari Sedana. The approaches used are the statute approach and the fact approach . The data used in this study consist of primary data and secondary data . Primary data were obtained through interviews with related parties at PT BPR Karya Sari Sedana and customers who entered into credit agreements. Secondary data were obtained through literature studies covering laws and regulations such as the Personal Data Protection Act , the Banking Act , and the Civil Code , as well as relevant books and scientific journals. Data collection techniques were carried out through interviews and literature studies . The data obtained were then analyzed using qualitative analysis to draw conclusions regarding legal protection for customers regarding personal data leaks in credit agreements at PT BPR Karya Sari Sedana.

3. Results and Discussion

Forms of Internal and External Regulation and Supervision of BPR Regarding Leakage of Customer Personal Data in Credit Agreements

Internal control is a monitoring system established within an institution or organization to maintain security and ensure smooth operations. This oversight aims to ensure that all tasks within the organization are carried out properly and in accordance with applicable regulations. The internal control system encompasses organizational plans, work methods, and various supervisory measures used to prevent misuse of assets, ensure the accuracy of information, and ensure that management policies are properly implemented.

In banking institutions, an internal control system is implemented throughout all operational activities. This system aims to detect errors, prevent deviations from established procedures, and improve oversight effectiveness. Monitoring can be conducted through specific evaluations, observation of employee behavior, or through accounting systems that provide warning signals for any discrepancies (Nurvana Ali et al., 2025).

Misuse of personal data is a violation of the law because it can involve criminal acts such as theft or fraud. Therefore, protecting personal data is crucial, especially in the banking sector, which stores a large amount of sensitive customer information. This protection depends not only on law enforcement but also on clear regulations and public awareness regarding personal data security.

Based on an interview with Mrs. Putu Hermawati, President Director of PT BPR Karya Sari Sedana , the bank has undertaken various efforts to protect customer data. These efforts include providing education and outreach regarding customer data confidentiality, both internally to employees and externally to the public. Furthermore, management regularly provides employees with knowledge updates on customer data management.

One system used to protect customer data is dual control , a monitoring system that involves more than one party in a service process. In this system, every request for customer data must be made by the customer in question, providing their true identity. Afterward, customer service will ask the customer to fill out a form and verify the data to ensure that the person requesting the information is truly the owner of the data.

Internal controls in banks also consist of two types: general controls and application controls . General controls aim to ensure the organization's environment runs smoothly, while application controls serve to prevent and detect errors or fraud in transaction systems. These controls ensure that all data entered, processed, stored, and reported has been properly processed and has received proper authorization (Ahadi, 2022).

In practice, customer data protection is regulated in various internal documents, such as circulars and standard operating procedures. However, several obstacles remain, such as unequal employee understanding of personal data management and a lack of public awareness of the importance of safeguarding personal data. This demonstrates the need for comprehensive and sustainable data protection.

Most data breaches occur due to human error, such as employees leaving important documents on their desks or duplicating documents without adequate security measures. To prevent this, banks implement various security policies, such as clear desk and clear screen policies, which prohibit employees from leaving important documents or customer data unsecured on computers.

Furthermore, the bank implements a limited access (need-to-know) principle , meaning only certain employees have the authority to access customer data. This arrangement is supported by a role-based access control (RBAC**)** system that limits access based on each employee's duties and responsibilities. Internal audits are also conducted periodically to ensure there is no misuse of data access.

The bank also conducts routine monthly training for employees on consumer protection and customer data management. If an employee intentionally or unintentionally leaks customer data, they may be subject to administrative, civil, or criminal sanctions, depending on the severity of the violation.

In addition, PT BPR Karya Sari Sedana also implements **an** Information Security Management System based on the international standard ISO 27001:2022 to ensure information security. This system aims to maintain the confidentiality, integrity, and availability of information, while protecting data from unauthorized access.

Protecting customer personal data is crucial for banks because it impacts public trust in banking institutions. Therefore, banks are committed to safeguarding customer data from unauthorized access, use, or disclosure. If a data breach occurs beyond the bank's control, the bank will immediately notify customers so they can take preventative measures to address potential risks.

External control is oversight conducted by external parties, either formally or informally, such as bookkeeping audits by accounting firms or public assessments. In the banking context, external control is essential to ensure that banks can optimally perform their functions: collecting and distributing public funds, supporting economic growth, and maintaining national stability for the welfare of the people.

Since the transfer of banking supervision from Bank Indonesia to the Financial Services Authority (OJK) , this independent institution has carried out regulation and supervision of the banking sector. The OJK has broad authority, including creating regulations, granting and revoking licenses, reviewing financial services industry reports, enforcing administrative sanctions, and investigating violations. Bank Indonesia continues to carry out its macroprudential oversight function, particularly regarding financial system stability, but the OJK now has the responsibility for microprudential oversight. The two institutions must work together to ensure the banking sector operates healthily, safely, and adheres to prudential principles (Nugraha et al., 2016).

Personal data breaches demonstrate that customer data is highly vulnerable to misuse. Leaks can lead to financial losses and undermine public trust in banks. Therefore, banks have a legal obligation to maintain customer data confidentiality and are responsible for any breaches. This also underscores the importance of external oversight by the Financial Services Authority (OJK) and Bank Indonesia (BI), as well as law enforcement in the event of violations.

According to Ms. Putu Hermawati, President Director of PT BPR Karya Sari Sedana, Bank Indonesia plays a role in regulating and overseeing data security at financial services institutions under its supervision, including payment system data and employee data. BI is also responsible for data security during inter-institutional sharing to prevent fraud. Externally, system improvements and reporting of cybercrimes are part of efforts to mitigate the risk of data breaches.

Legal protection for customer personal data only applies if there is a valid legal relationship between the customer and the bank. This relationship provides the basis for customers to assert their rights, as stipulated in the Banking Law and the Consumer Protection Law. To strengthen data protection, the Financial Services Authority (OJK) and Bank Indonesia (BI) need to establish strict implementing regulations, including protection standards and administrative sanctions for banks or third parties who violate them.

With the emergence of innovative digital services such as neobanks and online lending apps, the Financial Services Authority (OJK) needs to adjust regulations and strengthen technology-based oversight. OJK Regulation No. 6/POJK.07/2022 and Law No. 27 of 2022 concerning Personal Data Protection emphasize the principles of clarity, certainty, transparency, and data security. This clarity principle requires banks to provide customers with clear information about how data is collected, used, and stored, thus enhancing effective personal data protection.

Data protection practices have been established through a range of internal policies, including circular letters and standard operating procedures. Nevertheless, in actual implementation, not all employees demonstrate sufficient knowledge and competence to handle personal data in a professional and accountable way. At the same time, public awareness of personal data rights remains limited, which often leads to a lack of understanding of potential risks. Effective documentation practices and integrity in performing organizational duties are therefore essential. An evaluation of the internal control system at BPR Karya Sari Sedana—covering the control environment, risk assessment, information and communication, control activities, and monitoring—indicates that the system is generally functioning effectively.

However, the public's expectation of secure and reliable banking services cannot be fully realized unless data protection becomes a central priority in all service processes. This suggests that data protection initiatives must be carried out in a holistic and sustained manner.

Furthermore, the prevalence of data breaches caused by human error points to the need for improvements in human resource management. This challenge is also կապված with organizational culture, which has yet to fully recognize data protection as a strategic concern. The study highlights that personal data protection should be understood not only from a regulatory perspective but also through practical and operational implementation. In response, BPR Karya Sari Sedana has introduced measures such as Clear Desk and Clear Screen policies to reduce the risk of internal data leakage. Additionally, customer risk profiling—based on business characteristics and financial activities—is used to determine appropriate data maintenance intervals.

Despite these efforts reflecting the bank's commitment to data security, certain weaknesses persist, particularly in terms of consistent application and oversight of internal compliance. Accordingly, it is important to reassess the effectiveness of current systems, while also strengthening staff capabilities and adopting more advanced security technologies. Data breach incidents further emphasize the need for greater investment in cybersecurity infrastructure. Banks are required to implement up-to-date technologies and best practices to safeguard customer information from increasingly sophisticated threats. Although banks,

especially BPR Karya Sari Sedana, have taken steps to enhance their security systems following such incidents, maintaining this focus as an ongoing priority remains essential.

Bpr Karya Sari Sedana's Responsibility For Debtor Customer Data Leakage

Legal liability is the obligation of an individual or party to be accountable for their actions, especially if those actions result in harm to another party. In the relationship between a bank and its customers, this responsibility arises from an agreement . Through this agreement, the bank is obligated to provide secure financial services, including safeguarding and protecting customer personal data. If the bank's negligence results in harm to the customer, the bank can be held accountable, for example by providing compensation (Amir, 2021).

Personal data protection is also a crucial part of banking risk management . Banks not only need to implement technological security systems but also have clear policies regarding data management and raise employee awareness about maintaining customer data confidentiality. This is crucial because customer data often contains sensitive personal information that can be misused for crimes such as fraud or identity theft(Aritonang et al., 2025).

In practice, customers are often in a weaker position when disputes arise with banks. Therefore, legal protection of customer data is crucial to maintaining public trust in banking institutions. The relationship between banks and customers is based not only on law but also on trust . This public trust is what enables banks to collect funds from the public and provide various financial services.

Based on an interview with Mrs. Putu Hermawati, President Director of PT BPR Karya Sari Sedana , the use of customer personal data must be guarded with great care due to the numerous fraud cases involving banking data. Therefore, banks need to conduct regular security audits to ensure that data protection systems are running smoothly. Banks must also provide customers with clear information about how their data is used, stored, and protected.

Furthermore, banks are required to comply with applicable regulations, such as Law Number 27 of 2022 concerning Personal Data Protection (Pemerintah Pusat, 2022), which requires financial institutions to maintain the confidentiality of customer data. In the event of a data breach, banks must have clear response measures in place, including notifying affected customers and taking preventative measures to prevent a similar incident from recurring.

In the banking world, the principle of bank secrecy is also known , namely the bank's obligation to maintain the confidentiality of customer financial information. Theoretically, there are two views: the absolute theory, which states that banks must always keep customer data confidential under all circumstances, and the relative theory, which permits the disclosure of customer data under certain circumstances, such as for legal or state purposes(Novarianti et al., 2025).

To maintain data security, banks typically have Standard Operating Procedures (SOPs) that govern who can access customer data and for what purposes. Furthermore, banks are required to have internal control systems, conduct regular audits, and implement various security measures such as data encryption and access monitoring.

Banking regulations also emphasize that data security is the responsibility of the entire organization, not just the information technology department. If a bank is proven negligent

in protecting customer data, it may be subject to administrative, civil, or criminal sanctions in accordance with applicable law (Muhamad Naufal Aulia Azmi et al., 2024).

In the practice of personal data protection, there are several important principles, namely ensuring that the collected data **is** accurate , protecting data from unauthorized access, limiting data storage to only as long as necessary, and limiting data transfer to remain in accordance with data protection regulations. With legal protection, a good security system, and ongoing supervision, it is hoped that public trust in the banking sector can be maintained and the risk of customer personal data leaks can be minimized (Ilman Maulana Kholis, 2025).

Privacy violations through misuse of personal data are still rampant, particularly in the banking sector. Practices such as the exchange of customer data between institutions, the disclosure of transaction information to unauthorized parties, and the trading of data by third parties can harm customers (Rahmadani et al., 2024). Customer data is a critical asset for banks, and therefore banking institutions have an obligation to maintain the confidentiality and security of personal data.

Legal protection for customers encompasses both preventive and repressive dimensions. Preventive protection aims to prevent violations before they occur, while repressive protection is implemented through law enforcement if violations do occur. Customer trust in the bank is key, as a valid legal relationship provides the basis for customers to assert their rights(Aziz & S, 2025).

In Indonesia, data protection is regulated by the Personal Data Protection Law (PDP Law) and the Financial Services Authority Regulation (POJK). The PDP Law and POJK emphasize the principles of clarity, certainty, transparency, and data security. Data subjects have the right to access, correct, or delete misused data, while data controllers are required to manage information transparently and accountably. Violations can result in administrative, civil, or criminal sanctions(Nathasya, 2024).

Data breaches at rural banks, such as the sale of customer data by unscrupulous marketers, demonstrate the importance of internalizing data protection within banks. Banks are required to implement prudent principles, from account opening and customer data verification to secure information management. The Financial Services Authority (OJK) has an oversight role to ensure banks comply with regulations, including digital security systems and emergency response procedures in the event of a data breach (Udayana et al., 2025).

With technological advancements, the risk of data misuse increases, making legal protection and oversight crucial for safeguarding customer rights, security, and trust, while supporting the integrity of the banking system as a whole.

4. Conclusions

Legal protection for customers at PT BPR Karya Sari Sedana is carried out through internal and external supervision. Internally, the bank conducts regular audits and establishes clear responsibilities for each employee in managing customer data. Externally, supervision is carried out by the Financial Services Authority and regulated by Law Number 27 of 2022 concerning Personal Data Protection and OJK Regulation Number 6/POJK.07/2022. The bank's responsibility for customer data leaks arises when errors or negligence result in losses for customers. In such cases, the bank may be required to provide compensation and subject

to sanctions in accordance with the provisions of Law Number 27 of 2022 concerning Personal Data Protection.

References

Ahadi, L. M. A. (2022). Efektivitas hukum dalam perspektif filsafat hukum: Relasi urgensi sosialisasi terhadap eksistensi produk hukum. *Jurnal USM Law Review, 5*(1), 110–127.

Amir, M. F. (2021). Referensi 6. *Al-Amwal: Journal of Islamic Economic Law, 5*(1), 59–71.

Aritonang, L. M., Zyetwill, Z., & Handayani, R. (2025). Analisis hukum terhadap kebocoran data pribadi dan penyalahgunaan identitas dalam perbankan berdasarkan Undang-Undang Nomor 27 Tahun 2022 tentang perlindungan data pribadi. *Ranah Research: Journal of Multidisciplinary Research and Development, 7*(5), 3146–3158. https://doi.org/10.38035/rrj.v7i5.1665

Aziz, M. F., & S, S. A. (2025). Perlindungan hukum terhadap nasabah atas penyalahgunaan data pribadi oleh pihak bank di era digitalisasi perbankan, 8840–8852.

Kholis, I. M. (2025). Perlindungan data pribadi dan keamanan siber di sektor perbankan: Studi kritis atas penerapan UU PDP dan UU ITE di Indonesia. *Staatsrecht: Jurnal Hukum Kenegaraan dan Politik Islam, 4*(2), 275–299. https://doi.org/10.14421/t5sfe747

Azmi, M. N. A., Saifudin, H., Purba, C. T., Suryaningtyas, A., & Situmorang, U. S. (2024). Analisa kasus kebocoran data pada Bank Indonesia dalam sistem perbankan. *Jurnal Multidisiplin Ilmu Akademik, 1*(6), 448–458. https://doi.org/10.61722/jmia.v1i6.3267

Nathasya, H. (2024). No title. *Edu Research Indonesian Institute for Corporate Learning and Studies (IICLS), 5*(1), 70–80.

Novarianti, W. D., Meliala, A. P. P. S., Yusuf, N. A. S., & Melati, B. N. C. (2025). Kerahasiaan bank vs hak atas informasi: Mengurai konflik kepentingan dalam perlindungan data pribadi. *Jurnal Multidisiplin Ilmu Akademik, 2*(1), 103–114. https://doi.org/10.61722/jmia.v2i1.3180

Nugraha, F. S., Njatrijani, R., Studi, P., Ilmu, S., Hukum, F., & Diponegoro, U. (2016). Antara lain meliputi anjungan tunai, perubahan personal identification number (PIN), alamat rekening atau. *5*(11), 1–13.

Nurdin, A. R. (2018). Kajian peraturan perlindungan konsumen di sektor perbankan. *Jurnal Hukum & Pembangunan, 48*(2), 299–312. https://doi.org/10.21143/jhp.vol48.no2.1665

Ali, Y. N., Roesli, M., & Nugroho, B. (2025). Perlindungan hukum terhadap nasabah bank berkaitan dengan menjaga rahasia oleh bank. *PESHUM: Jurnal Pendidikan, Sosial dan Humaniora, 4*(6), 8943–8952. https://doi.org/10.56799/peshum.v4i6.11871

Pemerintah Pusat. (2022). *Undang-Undang Nomor 27 Tahun 2022 tentang pelindungan data pribadi*. https://peraturan.bpk.go.id/Download/224884/UU%20Nomor%2027%20Tahun%202022.pdf

Rahmadani, A. E., Pangestu, Y., & Halizhah, N. (2024). Perlindungan data pribadi di era digital: Tantangan dan solusi dalam sistem perbankan. *Media Hukum Indonesia, 2*(4), 180–186. https://doi.org/10.5281/zenodo.14060556

Tarigan, H. A. A. B., & Paulus, D. H. (2019). Perlindungan hukum terhadap nasabah atas penyelenggaraan layanan perbankan digital. *Jurnal Pembangunan Hukum Indonesia, 1*(3), 294–307. https://doi.org/10.14710/jphi.v1i3.294-307

Udayana, U., Klod, D. P., & Denpasar, K. (2025). Analisis regulasi perlindungan data pribadi. *Jurnal Media Akademik (JMA), 3*(7), 1–13.