P-ISSN 0853 – 6422 E-ISSN: 2621-3737
KERTHA WICAKSANA
Available Online At:https://ejournal.warmadewa.ac.id/index.php/kertawicaksana e-mail: info.kerthawicaksana@gmail.com

The Protection of Consumers' Data whose Financing Application Rejected by Financial Service Institutions

Suwinto Johan, Amad Sudiro, Rayhan Mohmad Athallah Hafiz S.
Faculty of Business, Universitas Presiden, Faculty of Law, Universitas Tarumanagara, Faculty of Law, Universitas Tarumanagara
suwintojohan@gmail.com

Published: 07/01/2023

How to Cite:
Suwinto Johan, Sudiro, A., Hafiz, R.M.A (2023) The Protection of Consumers' Data whose Financing Application Rejected by Financial Service Institutions *KERTHA WICAKSANA: Sarana Komunikasi Dosen dan Mahasiswa*. 17 (2), Pp 156-161. https://doi.org/10.22225/kw.17.2.2023.156-161

Abstract
Financial service institutions require financial service applicants' data for financial capability evaluation. The data may include financial information, personal details such as property ownership, tax records, and family data. The submission of the data does not guarantee approval as some applications can be rejected. This study explored the the protection of customers' data when their applications were denied. This normative juridical study regarded secondary data and library resources. The findings of this study highlighted the need for regulatory guidelines to protect customer data, particularly for those whose applications were rejected since their data could be misused by outsourced marketing personnel considering the absence of specific monitoring system. Even more, financial service institutions are not held accountable for such actions that occurred outside their scope of authority. In conclusion, regulatory measures must be established to protect and prevent unauthorized use of customers' data.
Keywords: *Financial Institution, Financial Institution, Financing Rejection*

Abstrak
Lembaga jasa keuangan membutuhkan data pemohon jasa keuangan untuk penilaian kemampuan keuangan. Data tersebut dapat mencakup informasi keuangan, detail pribadi seperti kepemilikan properti, catatan pajak, dan data keluarga. Pengajuan data tidak menjamin persetujuan karena beberapa aplikasi dapat ditolak. Studi ini mengeksplorasi perlindungan data pelanggan ketika aplikasi mereka ditolak. Kajian yuridis normatif ini mempertimbangkan data sekunder dan sumber pustaka. Temuan penelitian ini menyoroti perlunya pedoman peraturan untuk melindungi data pelanggan, terutama bagi mereka yang aplikasinya ditolak karena datanya dapat disalahgunakan oleh tenaga pemasaran outsourcing mengingat tidak adanya sistem pemantauan khusus. Terlebih lagi, lembaga jasa keuangan tidak dimintai pertanggungjawaban atas tindakan yang terjadi di luar kewenangannya. Kesimpulannya, langkah-langkah pengaturan harus ditetapkan untuk melindungi dan mencegah penggunaan data pelanggan yang tidak sah.
Kata Kunci: Lembaga Keuangan, Lembaga Keuangan, Penolakan Pembiayaan

I. INTRODUCTION

The mishandling of customer personal data by unscrupulous parties is a prevalent concern. The Financial Services Authority (OJK) has received 56 complaints from banking customers who have had their personal data compromised and misused Radar Malang, (2022), underscoring the potential for malicious actors to exploit such information. Notably, some clients have reported receiving email Tim Detik.com, (2022) notifications for credit payments that they did not authorize, despite the bills being specifically addressed to them by name. Moreover, several individuals have been contacted by online loan providers (pinjol) even though they have never availed themselves of their services Saputra, (2021). In response to these incidents, the OJK has emphasized the necessity of implementing regulations that protect customer

personal data, particularly in the financial industry C. A. Putri, (2020).

In order to obtain financing from financial service institutions, individuals are required to provide supporting data that demonstrates their eligibility for the funding. Funding serves as a crucial means of support for various developmental activities. The lending process involves the completion of a credit agreement between the lender and the borrower, resulting in the establishment of a legal relationship between the two parties Rahayu & Sildawati, (2021). The financial service institution evaluates the customer's data and determines whether to grant credit based on the Five C principle Aryanto & Widiatno, (2013), which consists of Character, Collateral, Capacity, Conditions, and Capital Sihotang & Sari, (2019).

The Protection of Personal Data (PDP) Law, Law no. 27 of 2022, recognizes two categories of personal data: specific data and general data. Specific data refers to health data and information, biometric data, genetic data, criminal records, children's data, financial data, and other data as specified by laws and regulations. General data encompasses personal information such as full name, gender, nationality, religion, marital status, and other data used to identify an individual. According to articles 8 and 9 of the PDP Law, individuals have the right to end the processing, deletion, and destruction of data related to themselves. They can also revoke their consent to the processing of their personal data. Article 16 outlines the various stages of personal data processing, which includes obtaining, collecting, processing, analyzing, storing, correcting and updating, displaying, announcing, transferring, disseminating, or disclosing, as well as deleting or destroying. Article 44 requires personal data controllers to destroy personal data once the retention period has expired, at the request of the data owner, except when it is necessary for the completion of legal proceedings or when the personal data has been obtained illegally.

Banking information security needs to be guaranteed to prevent cybercrime, as specified in several laws, including Law no. 11 of 2009 (which has been amended to become Law no. 19 of 2016) concerning Information and Electronic Transactions Fauziah & Apriani, (2021), Law no. 8 of 1999 concerning Consumer Protection, and Law Number 36 of 1999 concerning Telecommunications and Electronic Transactions. Banks are required to maintain the confidentiality of their customers' information and are prohibited from sharing it with third parties Haryono & Santoso, (2019). Failure to protect customer data may result in financial institutions being held accountable. This is especially true when offering insurance products through telemarketing. Bahagia, Rahayu, & Mansur, (2019) The Banking Law, Law Number 10 of 1998, mandates the application of bank secrecy in the banking industry. Fauziah & Apriani, (2021) Any employee of a financial institution who shares a customer's financial information may be subject to penalties. This is in violation of the Banking Law, POJK Number 1/POJK/07/2012 concerning Consumer Protection in the Financial Services Sector, and Bank Indonesia Regulation Number 22/20/PBI/2020 concerning Bank Indonesia Consumer Protection. Tompul, (2022) However, there are currently no regulations specifically addressing bank secrecy in the collection of data, so new regulations are required to address this matter. Marpi, Monied, & Fitryantica, (2021)

The use of AI in managing customer data can have negative consequences, and regulators are recognizing the need for new regulations to govern its use in banking activities involving customer data. Ayunda & Rusdianto, (2021) Protection of customer data is crucial, and there may be criminal penalties for violating data protection regulations. However, there are currently no specific rules governing the use of AI in this context. Bintoro, Rozh, & Sutanti, (2022) In regards to the protection of customer data from being sold, SE OJK Number 14 of 2014 concerning Confidentiality and Security of Data and/or Consumer Personal Information provides regulations to protect customer data. Sandi, (2019)

The Financial Services Authority (OJK) has issued Financial Services Authority Regulation (POJK) Number 1/POJK.07/2013 concerning Consumer Protection in the Financial Services Sector at the regional level. Despite this, implementation of the POJK has encountered challenges, particularly with regard to obtaining support from business actors in the financial services sector. R. N. Putri & Sulistiyono, (2022)

This study provides valuable insights into the challenges faced by financial institutions in

protecting customer data. The involvement of outsourced marketing personnel and the potential for data leaks highlight the need for strict policies and monitoring mechanisms to ensure compliance with data protection regulations and ethical standards. The research highlights the importance of providing training to outsourced employees to enhance their awareness of the importance of data security and their responsibilities in protecting customer data.

The findings of this study have implications for both financial institutions and policymakers. Financial institutions can use these findings to enhance their data management practices and improve their customer-centric approach to financial services. Policymakers can use these findings to develop and implement regulations and guidelines to enhance data protection and privacy in the financial services sector.

Furthermore, the research also highlights the potential for further studies on this topic. Future research can explore the effectiveness of different data management practices and policies and their impact on customer trust and satisfaction. Additionally, research can focus on the use of data analytics and artificial intelligence in improving data protection and privacy in the financial services sector.

Based on the description above, the following research questions were proposed.

1. How does customer data, especially of those who have been refused financing, leak in financial service institutions?
2. What process should financial service institutions implement to protect customer data?
3. What challenges do financial service institutions face in maintaining the confidentiality of customer data and preventing leaks?

II. METODE

The normative juridical research is regarded suitable in researching the confidentiality and protection of customer data in the financial industry. This method allows for an in-depth analysis of legal norms and principles related to customer data in the financial industry, as well as the synchronization of laws and regulations at the vertical and horizontal levels. By examining library materials, such as laws, regulations, and legal cases, the researcher can identify and analyze the legal frameworks that govern the confidentiality and protection of customer data in financial service institutions. This method also enables the researcher to provide recommendations for improvements or changes in existing legal frameworks to better protect customer data. Overall, the normative juridical research method is a valuable tool for researching legal issues related to the confidentiality and protection of customer data in the financial industry.

This study regarded various types of legal materials, including primary, secondary, and other sources. Secondary sources refer to literature reviews of different publications, while other sources provide explanations about the primary and secondary materials used. The data utilized in this study were collected from various sources, such as relevant laws and regulations, and information pertaining to customer data protection.

In this study, the statutory regulation approach was used, involving a comprehensive review of all relevant laws and regulations. This approach relies on statutory regulations to guide the research. The normative juridical method is used to examine, identify, and adapt to the pertinent laws and regulations. This type of research includes the use of primary legal materials, secondary legal materials, and other supporting legal materials. Primary legal materials such as the 1945 Constitution of the Republic of Indonesia and related regulations are utilized in this research. Secondary legal materials include literature in the form of legal journals, scientific books, legal theories, symposium/seminar proceedings, and scientific articles. Materials that explain primary legal materials and secondary legal materials are categorized as other legal materials (Johan, 2022). Qualitative method was employed in this research.

III. RESULT AND DISCUSSION

Source of Customers' Data

Financial service institutions frequently use customer data as one of the sources for offering financial products. Such offers through social media or telephone often cause public concerns. People may question the origin of their data and why they are being contacted by marketing representatives from financial service institutions as illustrated in Figure 1.

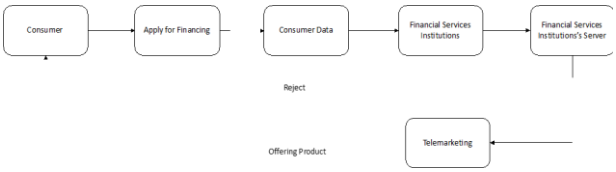

Figure 1 Process of Consumer Data in Financing Business

The PDP Law stipulates that the use of data requires the consent of the data owner. However, in reality, this is not always the case. The sources of data are often unknown, which makes it difficult for the public to trace the origin of data leakage. Furthermore, financial service institutions only use customer data obtained from their own databases for marketing purposes.

The use of data without the consent of the owner is a violation that may lead to sanctions under the PDP Law. However, in practice, financial service institutions still allow their sales force to use data without the owner's consent. There is also limited socialization regarding the PDP Law, and people often make appeals to those who contact them or reject their offers.

Apart from using internal data sources, financial service institutions may obtain customer data from unofficial sources. For example, customer data can be obtained from telephone numbers and customer names that are traded by various sources, including property agents and marketing agents.

Data Leaks in Financial Institution, Particularly the Data of Customers whose Credit Applications are Denied

One possible reason for customer data breaches is when an individual applies for credit or financing but is subsequently declined. In such instances, the customer's personal information is typically recorded in the financial institution's database, despite not being granted the credit or financing. Instead of leaving these individuals susceptible to data breaches, financial institutions should consider alternate solutions and propose financial products that are better suited to their financial condition.

This approach not only protects customer data but also creates a more customer-centric approach to financial services. Financial institutions can use customer data to analyze their financial situation and offer products and services that best meet their needs. This can include offering a lower credit limit or a different financing option that better suits their financial circumstances. Financial institutions can maintain customer loyalty and trust, while simultaneously reducing the risk of data breaches.

Moreover, financial institutions can implement a data retention policy to ensure that customer data is kept only for a specified period. After this time, the data is securely destroyed, eliminating the risk of data breaches. This policy should be communicated clearly to customers, and they should be informed of the time frame that their data will be stored. By doing so, financial institutions can create a more transparent approach to data management, which will build trust with customers and enhance the institution's reputation.

After a customer's credit application is declined, their data is typically retained by the financial institution and may be shared with the institution's sales representatives to offer alternative financial products.

In addition to complying with the PDP Law, financial institutions can also benefit from deleting or destroying the data of rejected customers. This reduces the risk of data breaches and improve their data management practices. This approach can also enhance customer trust and satisfaction as customers will appreciate the institution's commitment to protecting their data.

Furthermore, financial institutions can leverage data analytics and artificial intelligence to optimize their data management practices. By analyzing customer data, financial institutions can identify patterns and trends, which can help them tailor their financial products and services to better meet customer needs. This approach can enhance customer satisfaction and loyalty, which can lead to increased revenue and market share.

The Mandatory Process to Customer Data Protection by Financial Institutions

Financial service institutions must establish comprehensive policies to ensure the protection of customer data. In the event of any data leaks, the institution must announce the incident and impose sanctions on those responsible. Financial institutions must also inform customers if their data has been compromised as a result of the institution's processes. Such notification is crucial to enable customers to take necessary actions to protect themselves against potential identity theft or other adverse consequences.

Financial service institutions have a

responsibility to provide customers with guarantees for the data provided to them. They must emphasize that all data will be returned and destroyed in the event of a cancelled application. Such guarantees should be prominently displayed in the application process for credit or financing.

To protect customer data, financial service institutions must also establish robust information technology systems and work monitoring policies for staff with access to customer data. Regulators, such as the Financial Services Authority (OJK), should issue policies to guide financial service institutions in implementing these systems and policies. By providing customers with data protection guarantees and investing in secure information technology systems and work monitoring policies, financial service institutions can maintain customer trust and confidence in their services.

Challenges in Preventing Data Leaks in Financial Institutions

The importance of closely monitoring staff who interact with customers cannot be overstated for financial service institutions. Marketing staff, in particular, are a key area of focus, as they often have access to sensitive customer data that can be used for nefarious purposes. Outsourced marketing employees can be especially problematic, as they may not have a direct relationship with the institution and may be motivated to misuse customer data for their own gain. This can take the form of submitting fraudulent credit or financing applications to multiple institutions to receive incentives for approved applications, resulting in a significant breach of data protection regulations. To combat this issue, financial service institutions must take proactive steps to establish clear guidelines and monitoring systems for their outsourced employees. This includes training and awareness-raising programs to help outsourced employees understand the importance of data security and the potential consequences of misuse.

To prevent such abuses, financial service institutions must take proactive measures to establish clear guidelines and monitoring systems for their outsourced marketing employees. The institutions should thoroughly vet and screen their outsourced employees to ensure that they are trustworthy and comply with data protection regulations. Institutions must also provide training to their outsourced employees to improve their awareness of the importance of data security and the ethical standards they are expected to uphold.

Supervising outsourced employees can be challenging for financial service institutions, as they do not have direct control over these employees. However, institutions can establish strict policies and monitoring mechanisms to ensure that outsourced employees comply with regulations and ethical standards. Institutions must emphasize the importance of data security and provide training to outsourced employees on how to handle customer data with care. In cases where outsourced employees violate data protection regulations or engage in unethical behavior, financial service institutions can take legal action against them. However, it is important for institutions to establish clear policies and guidelines that clarify their responsibility in such situations to protect themselves from legal liabilities. Johan & Ariawan, (2022)

IV. CONCLUSION

Financial service institutions need to ensure the confidentiality and protection of customer data that is obtained daily from marketing personnel. They should clearly communicate to customers that their data will be kept confidential and destroyed once the transaction is completed or cancelled. This is mandated by the Personal Data Protection Act. However, monitoring the use of personal data is challenging for financial service institutions due to the involvement of outsourced marketers who may trade the data. More research can be conducted on the length of the financing application process, the required data for financing, and the potential for customer data leakage.

REFERENCES

Aryanto, R., & Widiatno, A. (2013). Prioritas Alternatif Keputusan Pada Analisis Kredit Motor. *Binus Business Review, 4*(1), 316–321.

Ayunda, R., & Rusdianto. (2021). Perlindungan Data Nasabah Terkait Pemanfaatan Artificial Inteligence dalam Aktivitas Perbankan di Indonesia. *Jurnal Komunikasi Hukum, 7*(2), 469–480. Retrieved from https://ejournal.undiksha.ac.id/index.php/jkh/issue/view/863

Bahagia, Rahayu, S. W., & Mansur, T. M. (2019). Protection Of Private Data Of Customers In Offering Insurance Transactions By Indonesia State Bank (Persero). *Syiah Kuala Law Journal*, *3*(1), 18–34.

Bintoro, V. S. A., Rozh, U., & Sutanti, R. D. (2022).

Tinjauan Yuridis Terhadap Tindak Pidana Penyalahgunaan Data Nasabah Oleh Perbankan Terkait Perlindungan Nasabah. *Diponegoro Law Journal*, *11*(3), 1–23.

Fauziah, I. S., & Apriani, R. (2021). Tinjauan Yuridis terhadap Perlindungan Nasabah Perbankan Yang Menggunakan Layanan Internet Banking. *Wajah Hukum*, *5*(2), 500–508. https://doi.org/10.33087/wjh.v5i2.557

Haryono, C. A., & Santoso, B. (2019). Kewajiban Bank Melaporkan Perpajakan Data Nasabah Berdasarkan Prinsip Kerahasiaan Bank. *Notarius*, *12*(1), 416–432.

Johan, S. (2022). Perbedaan Perlindungan Privasi Konsumen di Industri Keuangan dan Non-Keuangan. *Masalah Masalah Hukum*, *51*(3), 250–258.

Johan, S., & Ariawan, A. (2022). Correlation Financial Institutions, Customers and Employees Per Labour Law. *Arena Hukum*, *15*(1), 38–58. https://doi.org/10.21776/ub.arenahukum.2022.01501.3

Marpi, Y., Monied, D., & Fitryantica, A. (2021). Urgensi Konstitusional Perbankan Pada Kerahasiaan Nasabah Bagi Kepentingan Negara dan Kepentingan Privat. *Nalar Keadilan*, *1*(1), 30–43.

Marzuki, M. P. (2017). *Penelitian Hukum: Edisi Revisi* (Revisi). Retrieved from https://opac.perpusnas.go.id/DetailOpac.aspx?id=1409842

Putri, C. A. (2020). *OJK Khawatir Penyalahgunaan Data Nasabah, Minta DPR Bertindak*. Retrieved from https://www.cnbcindonesia.com/tech/20201111160413-37-201093/ojk-khawatir-penyalahgunaan-data-nasabah-minta-dpr-bertindak

Putri, R. N., & Sulistiyono, A. (2022). Menggugat Peran Otoritas Jasa Keuangan Dalam Perlindungan Data Nasabah Konsumen Jasa Keuangan Perbankan. *Privat Law*, *10*(April), 35–45.

Radar Malang. (2022). *56 Data Nasabah Disalahgunakan | Radar Malang Online*. Retrieved from https://radarmalang.jawapos.com/kriminal/17/09/2022/56-data-nasabah-disalahgunakan/

Rahayu, N. I., & Sildawati, S. (2021). Analisis Pemahaman Persepsi Nasabah Terhadap Kebijakan Relaksasi Kredit Diera Covid 19. *Prosiding Seminar Nasional Ekonomi ...*, *1*, 228–240. Retrieved from https://ejurnal.umri.ac.id/index.php/sneba/article/view/3061

Sandi, E. (2019). Pengawasan Otoritas Jasa Keuangan Terhadap Perbankan Sebagai Upaya Perlindungan Hukum Nasabah Atas Penjualan Data Nasabah Bank. *Jurnal Idea Hukum*, *5*(2), 1532–1543.

Saputra, A. (2021). Tidak Pinjam Pinjol Tapi Ditagih dan Diteror, Saya Harus Bagaimana? *Detik.Com*. Retrieved from https://news.detik.com/berita/d-5712898/tidak-pinjam-pinjol-tapi-ditagih-dan-diteror-saya-harus-bagaimana

Sihotang, B., & Sari, E. K. (2019). Restrukturisasi Sebagai Penyelamatan Kredit Bermasalah Pada Bank. *Seminar Nasional Pakar Ke-2*, (2), 1–6.

Tim Detik.com. (2022). *Data Pribadi Saya Disalahgunakan untuk Kredit, Apa yang Harus Saya Lakukan?* Retrieved from https://news.detik.com/berita/d-6325486/data-pribadi-saya-disalahgunakan-untuk-kredit-apa-yang-harus-saya-lakukan

Tompul, V. B. (2022). Data Nasabah Dibocorkan Oleh Oknum Pegawai Bank. *Binamulia Hukum*, *11*(2), 171–176. https://doi.org/10.37893/jbh.v11i2.723