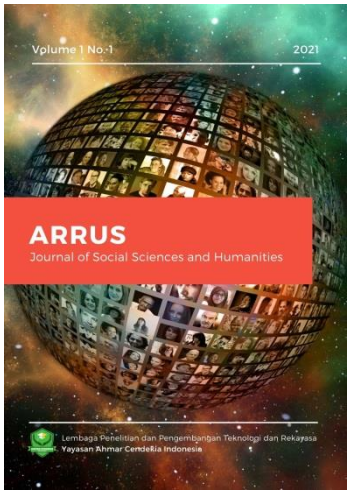
https://doi.org/10.35877/soshum2169

OPEN ACCESS

ISSN: 2776-7930 (Print) / 2807-3010 (Online)



*Corresponding author: Wulan Rannie B., University of Andalas, Padang City, 25175, Indonesia

E-mail: ranniebenny@gmail.com

RESEARCH ARTICLE

Legal Protection of Customer Personal Data in the Banking Sector

Wulan Rannie B.

University of Andalas, Padang City, 25175, Indonesia

Abstract: In banking, what becomes a bank secret is all forms of personal data about customers and their deposits. With the current technological advances, banks are expected to be able to provide faster, easier, and safer services in transactions process. However, it is undeniable that during the transactions process, a risk for both banks and customers of data theft is done by other parties. This research is legal research using normative juridical legal research or library legal research carried out by examining library materials or secondary research sources consisting of primary legal materials, secondary legal materials, and tertiary legal materials. Based on the research results, there are several rules that can protect personal data, that are Law No. 10 of 1998 concerning Amendments to Law No. 7 of 1992 concerning Banking, Financial Services Authority Regulation (POJK) No. 11/POJK.03/2022 dated 6 July 2022 concerning the Implementation of Information Technology by Commercial Banks, and Law No. 27 of 2022 dated 17 October 2022 concerning the Protection of Personal Data. Based on these regulations, it is clear that they cannot fully protect banks and customers from personal data leaks. In addition, there are no regulations with concrete steps to protect personal data so that banks can implement risk management in data protection.

Keywords: legal protection, customer data

1. Introduction

Technological developments have a major influence on human progress and welfare. This covers various fields, including the banking sector. Through the technology business activities and banking services, these are increasingly made easier and faster (Haliwela, 2023; Kulesza, 2018). The tendency of similarity in products and services offered by banks to customers requires the bank to provide a unique value proposition to maintain its existence. Higher quality service, coupled with the use of the best information technology are several reasons why customers choose certain banks (Haliwela, 2023; Haris Sanjaya & Arabella, 2023; Zuiderveen Borgesius & Poort, 2017).

Electronic banking (E-Banking) is a bank facility in this modern era that follows developments in technology and communication. Services available in E-banking include payments, transfers, history, and so on (Eddy Jusup, et al., 2023). In the marketing field, banking institutions have also built a special website (network) to carry out the E-Banking process, all of which aims to make it easier for customers to make transactions and obtain information about banking and banking products (Reza & Susanti, 2019).

Service innovation, collaboration with bank partners, and process automation are several things that banks must be concerned, especially in facing risks that may arise from any

https://doi.org/10.35877/soshum2169

ISSN: 2776-7930 (Print) / 2807-3010 (Online)

strategies formulated in the future. The implementation of e-banking is expected to provide convenience at a higher level than existing services. However, e-banking also increases the risks faced by banks, especially those related to operational risk, strategic risk, and reputation risk (David et al., 2016; Saputra et al., 2018; Setyowati & Prabowo, 2021).

The criminal act as the impact of this technological development is cyber-crime. One of the most popular cyber-crimes is Cracking. This is a technique for breaking into computer software and its security system for criminal purposes and leading to criminal acts. Cracking is very dangerous because it can steal data on a computer, leak information or destroy the security system (Wibowo et al., 2023).

Cybersecurity or Cyber Resilience is the practice of protecting important systems and sensitive information from digital attacks. The targets of these attacks are financial/money profits and sensitive information. Trust is the foundation of the financial services sector, so maintaining data security and confidentiality is very important for financial services organizations to maintain customer in the long term. Theft of employee, customer, and business data can threaten the credibility and integrity of financial institutions. Therefore, stakeholders need to focus on efforts to increase cyber resilience and maintain financial system stability .

In this current condition, there have been allegations of data leaks at Bank Syariah Indonesia (BSI). It is suspected that the LockBit Ransomware hacker group claimed responsibility for the cyber attack on BSI. LockBit stated that it hacked and stole 1.5 terabytes of personal data (DPR, 2023). Data consisting of name, cellphone number, address, account number, average account balance, transaction history, employment and account opening date is spread to be bought and sold on the dark web. As a result of this attack, the BSI system was paralyzed, disrupting BSI transactions on Automated Teller Machine (ATM) services, mobile banking, and internet banking errors for several days (Alley, 2023; Hadi et al., 2021; Martin, 2021).

Data which was successfully compromised by another party certainly made customers worried and reduced their trust in the bank. Banks must maintain the interests and trust of the public considering that most of the funds used by the Bank to carry out its business activities come from public savings entrusted to the Bank. For this reason, it is necessary to manage risk by applying the prudence principle in banking business activities (Aisjah et al., 2022).

Regarding what is meant by the prudential principle as stated in the provisions of Article 2 of Law number 10 of 1998 concerning banking (banking law), there is no official explanation. However, it can be stated that banks and the people involved in them, especially in making policies and carrying out business activities, they are obliged to carry out their respective duties and authorities carefully and professionally to gain the public's trust (Hemansyah, 2014).

In terms of personal data protection, more specifically, the government has passed Law number 27 of 2022 concerning personal data protection (UU PDP) in September 2022. However, for implementing regulations, the Ministry of Communication and Information (Kominfo) is still reviewing regulations in the form of presidential regulations (Presidential Decree) as well as implementing provisions of the PDP Law in the form of government regulations (PP).

Based on this description, the author is interested to study further what legal regulations can protect customers from personal data leaks entitled "Legal Protection of Customer Personal Data in the Banking Sector"

2. Research Methods and Materials

https://doi.org/10.35877/soshum2169

ISSN: 2776-7930 (Print) / 2807-3010 (Online)

In looking for solutions to the existing problems, researchers utilized normative juridical legal research or library legal research, namely legal research carried out by examining library materials or secondary research sources consisting of primary legal materials, secondary legal materials, and tertiary legal materials. These materials were arranged systematically, studied, then a conclusion is drawn in relation to the problem being studied. Normative legal research or literature includes (Soekanto & Mamudji, 2001) legal principles, legal systematics, the level of legal synchronization, both vertically and horizontally, comparative law, as well as legal history researches.

Based on this division, the legal research that the researcher has compiled is included as normative legal research on the level of legal synchronization, both vertically and horizontally.

In terms of writing specifications, the researcher used the analytical description method, namely linking the currently applicable regulations and relating them to the problems described above, linked to opinions based on research and findings from legal scholars currently in force which relate to the problems discussed by the researcher (Raharjo, 2014).

3. Results and Discussion

3.1. Legal regulations for the protection of customer personal data in banking

Banks as companies operating in the financial services sector absolutely need customer personal data to process customer transactions. This personal data is collected when customers open an account, get a loan, and when customers make transactions via debit cards, mobile banking and internet banking. The personal data will then be processed internally by the bank as well as by supervisors and third party vendors appointed by the bank.

Regulations in Indonesia regulate companies that build businesses by collecting sensitive data from the public for use by the company. Therefore these companies must understand the rules, principles and practices of personal data protection. In addition, the government also regulates the relationship between banks and customers who use bank services, especially in the case of customers providing very sensitive personal information and data in the banking and financial sector, and banks must be ready to apply the principle of confidentiality.

The Indonesian government has made regulations governing the protection of consumer personal data, including:

1) Law Number 7 of 1992 concerning Banking as amended by Law Number 10 of 1998 concerning banking (banking Law)

In the explanation of Article 29 paragraphs 3 and 4 of the Banking Law, it is stated that the relationship between banks and customers is based on a relationship of trust (*fiduciary* relationship). Customers give trust to the bank in storing their money by providing personal data that is confidential (unknown to the public).

In the banking sector, bank secrets as stated in the banking law are all information regarding depositors and their deposits. Bank secrecy is one of the elements that must be possessed so that the institution can gain customers' trust in storing money.

Protection of all savings customer data must be in line with the implementation of the precautionary principle. This is related to the bank's obligation not to harm customers who have entrusted their funds to the bank. One of them is by providing adequate infrastructure, technology management, and technological security in the banking business.

2) Financial Services Authority Regulation (POJK) No. 11/POJK.03/2022 dated 6 July 2022 concerning the Implementation of Information Technology by Commercial Banks

https://doi.org/10.35877/soshum2169

ISSN: 2776-7930 (Print) / 2807-3010 (Online)

As an institution tasked with regulating, supervising, examining, and investigating the financial services sector in Indonesia, the Financial Services Authority (OJK) must ensure that all activities in financial services are carried out in an organized, fair, transparent, and accountable manner. The OJK also aims to create a stable and sustainable financial system and protect the interests of consumers and society.

The POJK No. 11/POJK.03/2022 dated 6 July 2022 concerning the Implementation of Information Technology by Commercial Banks regulates banking information technology governance, information technology architecture, risk management, cyber resilience and security, use of information technology service providers, placement of electronic systems, data management, and protection of customer data. As the implementer of POJK No. 11/POJK.03/2022, the Financial Services Authority (SEOJK) Circular Letter Number 29/SEOJK.03/2022 dated 27 December 2022 was issued regarding Cyber Resilience and Security for Commercial Banks.

Banks are obliged to implement the principles of personal data protection in processing personal data, one of which is by determining the classification of data that constitutes personal data. Furthermore, banks must also obtain customer and/or prospective customer approval regarding providing data to third parties, which is carried out in accordance with the provisions.

The POJK No. 11/POJK.03/2022 stipulates that commercial banks must have adequate risk management in processing personal data. This risk management includes active supervision of the bank's directors and board of commissioners, the adequacy of policies, procedures and setting risk limits.

3) Law No. 27 of 2022 dated 17 October 2022 concerning Personal Data Protection (UU PDP)

As the companies operating in the financial services sector, bank absolutely needs customer personal data to process customer transactions.

This personal data are collected when customers open an account, get a loan, and make transactions via debit cards and Mobile Banking applications. The personal data will then be processed internally by the Bank and by third party providers and vendors appointed by the Bank.

The presence of Law No. 27 of 2022 concerning personal data protection brings a breath of fresh air, as well as an impact on the current processing of personal data. One of the mandates of this law is that companies are required to obtain legal and explicit consent to use personal data. It is important to ensure that the bank has obtained customer consent to use Personal Data, while ensuring that personal data is processed efficiently and securely to ensure data security and confidentiality.

Personal data (*Personal Identifiable Information*/PII) is data about natural persons who are identified or can be identified individually or in combination with other information, either directly or indirectly, through electronic or non-electronic systems.

Personal data is classified into two, namely general personal data and specific personal data. General personal data is personal data that contains similar information as personal data belonging to other individuals. Meanwhile, specific personal data is personal data that refers specifically to a particular individual and its processing may result in a greater impact on the subject of the personal data, including acts of discrimination and harm to the subject of the personal data. Example shown in Table 1.

In this case, the government of the Ministry of Communication and Informatics *(Kominfo)* is currently still drafting a Draft Government Regulation (RPP) regarding the protection of personal data, which will later become an instrument for establishing further regulations in implementing the PDP Law.

https://doi.org/10.35877/soshum2169

ISSN: 2776-7930 (Print) / 2807-3010 (Online)

This rules will later regulate in more detail the mandate of the PDP Law, which includes various provisions regarding personal data processing activities, including regarding the disclosure and analysis of personal data (*Personal Data Protection RPP Revealed, Check What's Missing* , n.d.).

Table 1. Example of Personal Data

General personal data	Specific personal data
Full name	Identity number (NIK/SIM/Passport)
Gender	Email/telephone number
Citizenship	Account/debit card/credit card number
Religion	Biometric data and genetic data
Marital status	Health information and criminal records
Transaction data	Financial data (amount of deposits, credit card data)
Birth mother's maiden name	Child data
Personal data combined to identify an individual	Other data is in accordance with the provisions of the law

3.2. Efforts made by customers and banks regarding suspected customer data leaks

In cyber-crimes, there are at least 2 (two) groups of victims in the banking system, namely: firstly, banking companies where there has been network damage and disruption as well as theft of customer data in the banking system. Secondly, banking customers whose data have been stolen.

One way of data theft carried out by cyber criminals is by sending Malware, Ransomware, and Viruses which have the aim of damaging the system, stealing confidential data or information, and obtaining illegal financial benefits from infected computers. This can come from activities while surfing in cyberspace, such as clicking on a link that turns out to be a trap or downloading and opening a file that contains a ransomware program. Malware, Ransomware, and Viruses can be detrimental and have a negative impact on the Bank's reputation, operations, finances, compliance, and legal challenges.

If a bank data leak occurs, responsibility does not only lie with the bank or the customer depending on the cause of the leak. Banks have a responsibility to maintain the security of customer data and protect their personal data, as well as customers who are also required to care about protecting their personal data, such as the confidentiality of passwords or personal identification numbers (PIN).

There are customer rights and obligations that arise if this event occurs as follows (Kusuma, 2019):

Customers' rights:

a) Customers have the right to receive protection for savings or accounts held at a bank. Based on Article 29 paragraph (3) Law No. 8 of 1999 concerning consumer protection and the precautionary principle.
b) Customers have the right to obtain information relating to the possible risk of loss in connection with customer transactions carried out through the bank, based on Article 29 paragraph (4).
c) Customers have the right to receive compensation for lost or stolen funds or accounts from the bank holding the deposit rights. Moreover, there is also legal protection that customers who save funds receive against all risks of loss arising from a policy or arising from business activities carried out by the bank. Based on Presidential Decree No. 26 of 1998 concerning Guarantees for Commercial Bank Liabilities.

Obligations:

a) Customers are obliged to actively provide information regarding irregularities or losses they have suffered to the bank, so that it can be processed further.

https://doi.org/10.35877/soshum2169

ISSN: 2776-7930 (Print) / 2807-3010 (Online)

b) Customers are also obliged to provide information in the judicial process as a witness if a legal problem occurs, in this case, the crime of account theft (*carding*) from the bank concerned.

The bank's responsibility regarding suspected customer data leaks is crucial in protecting customer personal data. The following are some responsibilities that can be associated with this situation:

a) Addressing security; Banks have a responsibility to ensure that their data security systems continue to be improved, including implementing appropriate policies and protocols to protect customers' personal data. This involves regular monitoring, security testing, and relevant technology updates.
b) Prevention and Detection; Banks must have strong systems and infrastructure to detect and prevent unauthorized access to customer data. This can include implementing security layers such as *farewalls,* data encryption, and intrusion detection systems.
c) Quick Response and Transparency; If there is a suspected customer data leak, Bank must provide a quick and transparent response to affected customers. They must provide clear information about the incident, the steps taken to resolve the problem, and provide assistance to protect customers from possible data misuse.
d) Carrying out investigations and reporting; Banks have the responsibility to carry out thorough investigations regarding suspected customer data leaks. They must report these incidents to the competent authorities, such as the Banking Supervisory Agency or similar institutions in accordance with applicable laws.
e) Providing relief and recovery; Apart from providing preventive measures, banks must also provide assistance to customers who are victims in recovering losses that may occur due to data leaks. This could be financial recovery, identity monitoring, or necessary legal assistance.
f) Increased awareness; Banks also have a responsibility to increase customer awareness about data security threats and how to protect themselves. This can be done through educational campaigns, providing advice on digital security practices, and ensuring customer compliance with applicable security policies.

In accordance with Article 46 of the PDP Law, if there is a failure to protect customer personal data, the bank is obliged to provide written notification no later than 3 x 24 (three times twenty four) hours to the customer and the bank supervision agency.

The Bank applies the principles of controlling the security of Customer data and transactions from Digital Banking Services in every electronic system used, including but not limited to:

a) Banks are obliged to ensure that information security is implemented effectively and efficiently.
b) Information security is carried out on aspects of human resources, technological processes, and physical or environmental aspects in the overall implementation of instructional technology.
c) Banks are required to have a disaster recovery plan.
d) Banks are obliged to ensure that disaster recovery plans are implemented so that the continuity of Bank operations keeps continue when a disaster occurs and/or disruptions to the IT facilities used by the Bank.

4. Conclusion

Information technology (IT) in banks has an impact on the development of digital-based banking products, which make it easier for customers to obtain information, communicate, and carry out banking transactions. On the other hand, the implrmrntation of information technology has an impact on increasing risks and vulnerabilities in the Bank's operational activities. This requires the Bank to implement Information Technology Governance in

https://doi.org/10.35877/soshum2169

ISSN: 2776-7930 (Print) / 2807-3010 (Online)

order to minimize risks and optimize business value from the use of Information Technology.

Therefore, managing Information Technology is not only the responsibility of the Information Technology Work Unit but also all elements of the Bank, starting from business strategy planning (Long Term Plans, Medium Term Plans, Work Plans, and Company Budgets as well as Bank Business Plans), support for infrastructure provision, technology management that follows business trends, adequate technological security, accurate recording, fast transaction processes, as well as communication with the wider community which will be the scope of the Bank's operational policies. Furthermore, to support the Bank's activities, it is expected that the government can make regulations as guidelines for all Bank officials and employees in implementing Information, Data, and Digital Technology Governance based on regulations, the Bank's prudential principles, and good banking principles.

References

Aisjah, S., Prabandari, S. P., & Hamid, W. (2022). Sustainability Factors of Sharia Banks in Indonesia. *Quality - Access to Success*, *23*(190). https://doi.org/10.47750/QAS/23.190.40

Alley, I. (2023). BOFIA 2020 and financial system stability in Nigeria: Implications for stakeholders in the African largest economy. *Journal of Banking Regulation*, *24*(2). https://doi.org/10.1057/s41261-022-00192-6

David, B., Abel, F., & Patrick, W. (2016). Debit card and demand for cash. *Journal of Banking and Finance*, *73*. https://doi.org/10.1016/j.jbankfin.2016.08.009

DPR. (2023). Sukamta Minta BIN, BSSN, Polri, dan Kominfo Terlibat Selesaikan Masalah Dugaan Peretasan BSI. *Dpr.Go.Id*.

Eddy Jusup, Endang Juju, Nurochani, N. (2023). *Strategi Pengembangan Layanan E-Banking Syariah*. 62.

Hadi, N., Wayan, S., Wibowo, R., & Wardhono, A. (2021). An Empirical Study of Financial Inclusion and Financial System Stability in ASEAN-4. *Journal of Asian Finance*, *8*(7).

Haliwela, N. S. (2023). The Essence of Legal Protection of Personal Data of Customers In Banking Transactions. *SASI*, *29*(3). https://doi.org/10.47268/sasi.v29i3.1528

Haris Sanjaya, U., & Arabella, R. (2023). Legal Protection of Consumer Data on E-Commerce Platforms with Cash on Delivery (COD) Systems. *KnE Social Sciences*. https://doi.org/10.18502/kss.v8i9.13386

Hemansyah. (2014). *Hukum Perbankan Nasional*. 59.

Kulesza, E. (2018). The protection of customer personal data as an element of entrepreneurs' ethical conduct. *Annales. Etyka w Życiu Gospodarczym*, *21*(7). https://doi.org/10.18778/1899-2226.21.7.02

Kusuma, M. J. (2019). *Hukum Perlindungan Nasabah Bank*. 54.

Martin, V. (2021). Central Bank digital currencies. *Bankarstvo*, *50*(3). https://doi.org/10.5937/bankarstvo2103109m

Raharjo, B. (2014). Akhir Dering Telemarketing. *Republika*.

Reza, H. K., & Susanti, M. (2019). *Keuangan Digital*.

RPP Perlindangan Data Pribadi DIberberkan, Cek Apa Saja Kurangnya. (n.d.).

Saputra, N., Abdinagoro, S. B., & Kuncoro, E. A. (2018). The mediating role of learning agility on the relationship between work engagement and learning culture. *Pertanika Journal of Social Sciences and Humanities*, *26*(T), 117–130.

Setyowati, R., & Prabowo, B. A. (2021). Sharia principles in the financial services authority regulation on dispute settlement alternatives. *Sriwijaya Law Review*, *5*(1). https://doi.org/10.28946/slrev.Vol5.Iss1.603.pp56-70

https://doi.org/10.35877/soshum2169

ISSN: 2776-7930 (Print) / 2807-3010 (Online)

Soekanto, S., & Mamudji, S. (2001). *Penelitian Hukum Normatif : Suatu Tinjauan Singkat*.

Wibowo, S. H., Irawan, J. D., S, W., Winardi, B., Santoso, L. W., Sari, D. P., Dewantara, R., Jamaludin, Nurhadi, Sihombing, F. A., Aulia, A. P., Heryana, N., & Kurnaedi, D. (2023). *Cyber Crime di Era Digital. December 2022*, 223.

Zuiderveen Borgesius, F., & Poort, J. (2017). Online Price Discrimination and EU Data Privacy Law. *Journal of Consumer Policy*, *40*(3). https://doi.org/10.1007/s10603-017-9354-z