JULIAN
Journal of Law Education and Legal Science
E-ISSN: 3110-3227 | P-ISSN: 3123-478X
Vol. 1. No. 2 December 2025. Pages. 69-76

# Study On Sharia Bank Customer Data Leak Indonesia In 2023 : Perspective Of The Data Protection Law Personal No. 27 Of 2022

**Febri Puji Lesmana[1]✉, Moh. Wakid[2], Ahmad Syauqi Bawashir[3], Mohammad Ramdan[4], and Rahmad Ready Kurniawan[5]**

Febrilesmana69@gmail.com[1], moh.wakid@unibamadura.ac.id[2], ongq97@unibamadura.ac.id[3], ramdan25@unibamadura.ac.id[4], and rahmadreadykurniawan@unibamadura.ac.id
[1] Business Law, Bahaudin Mudhary University Madura, Indonesia
[2] Faculty of economics and business, Bahaudin Mudhary Madura University, Indonesia
[3] Faculty of economics and business, Bahaudin Mudhary Madura University, Indonesia
[4] Business Law, Bahaudin Mudhary University Madura, Indonesia
[5] Faculty of economics and business, Bahaudin Mudhary Madura University, Indonesia

Keywords: Digital Banking, Data Leakage, Cybersecurity, PDP Law, Bank Syariah Indonesia

Submitted: 23/12/2025
Revised: 30/12/2025
Accepted: 31/12/2025

**Abstract**

The development of digitalization in the banking sector has brought ease of access to financial services through digital banking, but it has also increased cybersecurity risks. In May 2023, Bank Syariah Indonesia (BSI) experienced a data leak incident due to a ransomware attack by the LockBit 3.0 group, which revealed weaknesses in the data security system and caused potential losses for customers. This study uses a juridical-normative method to analyze the implementation of the Personal Data Protection Law (PDP Law) No. 27 of 2022 in handling these cases. The results of the study show that BSI as a data controller has a legal obligation to maintain the security of customer data, as stipulated in Article 46 of the PDP Law. However, BSI's delay in providing notifications, lack of information transparency, and negligence in ensuring the protection of personal data indicate non-compliance with these regulations.

**Author Correspondent:**
Febri Puji Lesmana
Busines Law, Bahaudin Mudhary Madura University, Indonesia
Jl.Raya Lenteng, No. 10, Batuan, Sumenep - Madura
Email: Febrilesmana69@gmail.com

## INTRODUCTION

Technology has undergone significant developments in recent decades, creating various innovations that change the way humans interact, work, and live their daily lives. Especially information technology which has become the backbone of digital

transformation in various sectors, including government, education, and financial services. With the presence of technologies such as cloud computing, artificial intelligence (AI), and big data, the process of processing and storing information has become faster, more efficient, and globally connected.

One of the sectors that dominates the use of technology the most is the banking sector. The banking sector utilizes technology to facilitate efficient banking access through online platforms often known as digital banking which include mobile banking applications, blockchains, and electronic payment systems. With digitalization in the banking sector, it allows people to access financial services only through mobile devices, bringing unprecedented convenience. Based on data from Bank Indonesia, it was revealed that in 2023, the value of digital banking transactions was recorded at IDR 58,478.24 trillion or grew by 13.48 percent Year On Years. (Source: Scott, 2023)

The growth of digital banking transactions that presents the digitization of transactions shows that technology plays an important role in the banking sector and people's daily lives, however, along with the high rate of transaction digitization, threats to digital security are also increasing. Indonesia is one of the countries that is vulnerable to cyber attacks. Based on the 2018 Global Cybersecurity Index (GCI) report released by the International Telecommunication Union (ITU), Indonesia is ranked 24th out of 194 countries in terms of readiness to face cyber attacks. (International Telecommunication Union, 2018)

This position shows that despite progress in digitalization, Indonesia's cybersecurity level still needs to be improved to protect people's digital transactions and personal data. The threat of cyberattacks such as ransomware, phishing, and data breaches is increasingly alarming, especially for the financial sector, which is one of the main targets of hacking. The report from the Interpol ASEAN Cyberthreat Assessment 2023 also revealed that Indonesia is among the countries with the highest level of cybercrime incidents in the Southeast Asian region. (Nikita Dewi Kurnia Salwa, 2024).

As a result, various potential losses, both financially and reputationally, lurk in the digital banking sector and the people who are victims. The impact is not only felt by individuals, but also affects economic stability and public trust in digital services. This threat poses a major challenge for governments, financial institutions, and digital service providers to ensure the security of the systems they use.

Various cases of data leaks due to cybercrime in the banking sector have occurred, such as in 2021 there was a data leak at Bank Indonesia (CNN Indonesia.com), (CNN Indonesia, 2022b) in 2018 there was a data leak at Bank Negara Indonesia (CNN Indonesia.com), (CNN Indonesia, 2022a) in 2020 there was a data leak at Citibank (Antaranews.com). (Antara News, 2013) The most recent data leak case is the BSI bank data leak case. This case occurred in May 2023, the cybercrime category that occurred was Ransomware. According to Safitri, K.A (2023) Ransomware is a cyberattack that attacks operational systems. banks thus causing digital banking services such as mobile banking and websites to be inaccessible for several days. This attack has had a major impact on customer activities, especially those who rely on digital banking services. In 2023, based on data released by BSI, the number of bank customers will reach 19.2 million. (Hanif Reyhan Ghifari, 2023).

Cybercrime cases that occur result in customer data leaks, this data leak causes the personal information of a number of customers to be threatened. With the threat that has emerged, regulation and strengthening of the data security system is increasingly urgent, especially in protecting individual rights to personal data security. In this context, the Personal Data Protection Law (UU PDP) No. 27 of 2022 is very relevant, especially in dealing with data leak cases that occurred at Bank Syariah

Indonesia (BSI). The Personal Data Protection Law (PDP Law) No. 27 was passed on October 20, 2022. This law is a regulation that aims to provide protection for individual personal data in Indonesia, regulating the way personal data is collected, used, and processed by various parties, including government and private institutions. This regulation is particularly important in the context of the increasing use of digital technology and threats to data privacy and security, as seen in the case of data leaks at Bank Syariah Indonesia (BSI).

PDP Law No. 27 of 2022 provides a clear legal framework for the protection of personal data, in PDP Law No. 27 of 2022 article 27 establishes the responsibility for data managers, including financial institutions, in maintaining the security of customer information. In the case of BSI, where a customer's personal data is leaked, the implementation of this regulation can help direct appropriate mitigation measures to avoid similar incidents in the future. The PDP Act also emphasizes individuals' rights over their personal data, such as the right to access, correct, and delete irrelevant information. The implementation of this law at BSI will not only increase transparency in data management, but will also build customer confidence in banks' ability to protect their sensitive information. Thus, through strengthening data security systems and compliance with the PDP Law, the banking sector, including BSI, can better face cybersecurity challenges and protect customer rights in the digital era. Overall, reviewing the PDP Law No. 27 of 2022 is not only important for legal compliance, but also as part of a risk mitigation strategy in dealing with increasingly complex and evolving cybersecurity threats.

## RESEARCH METHODS

This research was conducted using the juridical-normative method This approach is considered the most appropriate because the research is focused on how to implement the PDP Law No. 27 of 2022 on the data leak of Bank Syariah Indonesia based on the applicable legal provisions in Indonesia. In this case, the legal approach is the main framework to understand how existing regulations regulate banking obligations, as well as the extent to which these regulations are able to provide protection for customers' personal data. The data used in this study is secondary data, which includes written legal sources such as laws and regulations, legal literature, and various relevant academic journals. The regulation that is the main focus of the research is Law Number 27 of 2022 concerning Personal Data Protection, which regulates the scope of personal data, data rights and subjects, data management obligations, supervision and sanctions, and data security in this case of Bank Syariah Indonesia customers. Personal Data Protection Law (PDP Law), which provides a more comprehensive legal framework related to the management and protection of personal data.

## RESULTS AND DISCUSSION

### Implementation of The Fulfillment of Bank Sharia Indonesia's Obligations Based on PDP Law No. 27 Of 2022 In an Effort to Respond to Data Leak Cases

As a data controller, Bank BSI has an obligation to be responsible for the security of its customers' personal data. A personal data controller is any person, public body and international organization that acts individually or jointly in determining the purposes and exercising control over the processing of personal data. (Article 1 Paragraph 5, Law of the Republic of Indonesia Number 27 of 2022, n.d.) Based on PDP Law No. 27 of 2022 Article 46, there are alleged obligations that must be fulfilled by Bank BSI in the event of a personal data protection failure. (Article 46, Law of the Republic of Indonesia Number 27 of 2022, n.d.) The obligations contained in the article contain the obligation of the data controller to notify or

deliver written notice to personal subjects and institutions in the failure of personal data protection and must notify detailed information about the personal data leaked, the time and manner of the leak and the handling efforts within 3 x 24. In the case of the BSI Bank data leak in the ransomware attack, BSI Bank was late in delivering the notification. Based on CNN Indonesia (2023), BSI claims that the paralysis of systems and services is caused by the maintenance process. (CNN Indonesia, 2023) If the reason is valid, BSI should have taken better communication measures, including providing clear explanations to customers about the risks that may arise.

This action is important to build customer trust in the bank, as well as to comply with applicable legal provisions. In addition, the delay in notification by BSI shows that this obligation is not optimally fulfilled, which has the potential to cause legal consequences and losses for customers. Delays in notifying customers have a significant impact. Customers who are not informed about the data leak do not have the opportunity to protect themselves from potential identity theft or data misuse. For example, customers may suffer financial losses due to unauthorized transactions or fraud that exploit leaked information. Therefore, the role and responsibility of BSI as a data controller in this situation is crucial. In addition to the obligation to inform, the PDP Law also regulates the obligation of data controllers to recover lost or leaked personal data. In the case of BSI, such recovery measures are important to guarantee that the leaked data is not further misused. BSI needs to demonstrate a commitment to improving its security system and take steps to prevent similar incidents in the future. In addition to the delay in the information provided, BSI also committed negligence because it did not provide complete information regarding data leaks, such as the type of data that was leaked, when and how the leak could occur. The public or their customers found out about the data leak through lockbit social media uploads, this was due to the delay in the announcement made by BSI bank. This data leak incident has been experienced by BSI since May 8, but clarification was only given by the Ministry of Communication and Information on May 22, 2023.

**BSI Bank Legal Responsibility for Data Leaks**

Based on article 57 of the PDP Law No. 27 of 2022, if it is proven that there is a violation of the provisions of the article listed in article 57 paragraph (1), the data controller can be subject to administrative sanctions. In this context, the application of administrative sanctions against BSI requires proof that the elements of violations as stipulated in the PDP Law have been met. The first element is the existence of a clear legal relationship between BSI as the Personal Data Controller (PPDP) and the customer as the data subject. This relationship creates a legal obligation for BSI to ensure the security of customers' personal data that they have collected and managed. As a bank operating under the regulation of the Financial Services Authority (OJK), BSI is responsible for protecting customer data in accordance with the applicable principles of prudence and legal protection. The second element that must be fulfilled is the existence of personal data processing activities by BSI. Customers' personal data, such as names, account numbers, addresses, and other financial information, are processed by the bank for operational and service purposes. This data processing includes the process of collecting, storing, using, and deleting data. In this case, the data leak indicates that there is a security gap in the management of personal data carried out by BSI.

Furthermore, the third element is the leakage of customer personal data due to the acts or negligence of BSI. These leaks can occur due to a cyberattack that exploits system vulnerabilities, or due to the lack of adequate data security protocols in place by banks. Based on the data leak incident experienced by Bank Syariah Indonesia (BSI), a number of evidence shows that there is an element of negligence in the protection of customer personal data. The ransomware attack by the LockBit 3.0 group managed to steal about 1.5 terabytes of sensitive data, including customer information such as names, account numbers, balances, and transaction history. Other data includes

financial and legal documents, as well as BSI internal system access passwords. This omission is evident in the security aspect of the system, where BSI was unable to prevent the attack even though the hacker group had reportedly been on their network for two months before the attack occurred. This shows the potential lack of adequate monitoring and response systems to cyber threats. (Balqis Fallahnda, 2023) The fourth element is that the data leak results in losses or potential losses for customers. These losses can be identity theft, illegal access to bank accounts, or misuse of data for criminal purposes. The hackers had asked for a ransom of IDR 295 billion before finally customer data was published on the internet black market, (Lavinda, 2023) which could cause further losses for individuals and companies. This causes potential threats to customer privacy and security are enough to pose legal risks for BSI as the party responsible for the management of personal data.

The BSI data leak case also provides an important lesson about the importance of good personal data governance in the digital era. In the face of increasingly complex cyber threats, companies, especially in the banking sector, need to adopt more advanced data security technologies and systems. Failure to protect data not only damages a company's reputation but also creates distrust among customers. The application of administrative sanctions against BSI can include various actions, such as the imposition of administrative fines, written reprimands, or obligations to improve the data security system. In addition, the regulator may also recommend a thorough audit of BSI's data management system to ensure that the data protection policy has been improved according to the standards set out in the PDP Law. However, administrative sanctions are not the only step that needs to be taken. Recovery steps for affected customers must also be a priority. BSI may provide identity protection services or financial compensation to customers whose data has been misused. This approach is important to restore customer trust and demonstrate BSI's commitment to responding to these incidents responsibly.

As the latest solution, BSI needs to implement artificial intelligence (AI) technology to detect and prevent data leaks early. AI systems can monitor suspicious activity in real-time and provide alerts before a breach occurs. In addition, BSI can adopt a zero-trust architecture strategy that puts any data access under strict verification, thereby reducing the risk of exploitation by unauthorized parties. Not only that, but collaboration with third parties such as leading cybersecurity companies can provide a proactive approach to managing digital threats. Training for employees must also be improved to build a stronger data security culture. Through these measures, BSI can demonstrate concrete efforts in ensuring that similar incidents will not be repeated in the future.

In terms of law enforcement, this case also underscores the need to evaluate and strengthen existing regulations. The government can formulate the main law enforcement issues in such cases, including:

1. The absence of a fast and responsive legal mechanism in taking action against companies that fail to protect personal data. The solution that can be taken is to speed up the investigation process and impose sanctions, so that there is a deterrent effect for the perpetrators of violations.
2. Lack of standard technical guidance for data protection, particularly in the banking sector. Law enforcement can work with regulators to create more specific and technical policies, such as risk-based data protection guidelines.
3. Lack of periodic supervision and evaluation of the implementation of the PDP Law. The government can establish an independent supervisory body that

focuses on the management and protection of personal data, so that supervision is more focused and accountable.

With these legal steps, it is hoped that data leak incidents such as the BSI case can be handled with a more systematic approach, while encouraging the improvement of data governance standards in Indonesia.

**Evaluation of Bank BSI's Obligations as a Data Controller According to Article 39 of the PDP Law of 2022 in Ensuring That There is no Unauthorized Access**

The data leak case at Bank BSI shows a violation of Article 39 of the PDP Law. In this incident, the cyberattack resulted in the theft of customers' personal data, causing significant losses. Article 39 Paragraph 1 of PDP Law No. 27 of 2022 regulates the obligation to prevent unauthorized access to personal data. (Article 39 Paragraph 1, PDP Law No. 27 of 2022, n.d.) In the case of data leakage of Bank BSI, further analysis can be made regarding the implementation of Bank BSI's obligations in data security. Based on this article, it is known that in the case of this data leak, BSI can be concluded that BSI bank has failed to implement adequate security measures to protect customers' personal data. A successful ransomware attack indicates a loophole in the security system that should be protected in accordance with the provisions of Article 39 paragraph 1 As a data controller, Bank BSI has the responsibility to ensure that customer data is protected from unauthorized access. Although Bank BSI has an information security team or Chief Information Security Officer (CISO) and implements a 128-bit Secure Socket Layer (SSL) encryption technology system that protects communication between customer devices and the time out session method where after three minutes of inactivity, access can no longer be activated and must be reactivated, this data leak shows that Bank BSI's security system is still ineffective.

Some of the things that cause bank security to be hacked by irresponsible parties are (1) the existence of unlayered security. In protecting the security of the database server, it is necessary to have layered security, for example, a firewall which can play a role in controlling the access or entry and exit activities of parties from the database server. (2) Data backup, data backup plays an important role in anticipating cybercrime or other unexpected events. (3) Lack of a plan to anticipate attacks (crisis preparedness). Anticipation of cybercrime must be prepared to know what actions must be taken in the event of a cyber attack. (4) Lack of supervision from management. Supervision from management plays an important role in ensuring policy compliance in the security system that has been implemented to minimize weaknesses in internal control over the use of the security system or acts of fraud and negligence. (Jonathan Jordan Sianipar & Marta Solavide Naibaho, 2024).

## CONCLUSIONS AND SUGGESTIONS

### Conclusion

The case of data leakage at Bank Syariah Indonesia (BSI) due to a ransomware attack is one of the real examples of threats to data security in the digital era. This case highlights the importance of strengthening data security systems in the banking sector, especially in the face of increasingly complex cybercrime challenges. The implementation of the Personal Data Protection Law (PDP Law) No. 27 of 2022 is very relevant to ensure the protection of customer rights and support good data governance. The PDP Law regulates various data controller obligations, such as notifying data subjects within 3x24 hours after the leak occurs and efforts to recover the leaked data. However, in the case of BSI, this obligation has not been fully met, as can be seen from the delay in notification and lack of transparency regarding the type of data that is leaked. This has the potential to cause financial and non-financial losses for customers

and reduce trust in banking institutions. Legally, BSI's responsibilities include fulfilling data protection obligations, improving security systems, and providing compensation to affected customers. This case is an important lesson for the banking sector to improve digital security infrastructure and comply with applicable regulations to protect people's personal data.

**Suggestions**

1. For Indonesian Sharia Banks and Banking Institutions

Banks are advised to increase compliance with the PDP Law No. 27 of 2022 by strengthening the personal data security system, both in terms of technology, human resources, and internal governance. Banks also need to conduct regular data security audits, develop emergency response procedures for data leaks, and ensure transparent notification and recovery mechanisms to customers in the event of data leak incidents.

2. For the Government and Regulators

The government, together with the Financial Services Authority (OJK) and related agencies, need to strengthen supervision and law enforcement of the implementation of the PDP Law in the banking sector. More detailed technical regulations and implementation guidelines are also needed so that the obligations of personal data controllers can be applied uniformly and effectively, as well as the provision of strict sanctions for violations to provide a deterrent effect.

3. For Customers

Customers are advised to further increase awareness in protecting personal data, understand their rights as data subjects as stipulated in the PDP Law, and actively report if they find indications of misuse or leakage of personal data. Customer awareness and participation are an important part of creating a comprehensive data protection system.

4. For the Next Researcher

The next research is expected to examine more deeply the effectiveness of the implementation of sanctions in the PDP Law, the mechanism of bank legal accountability for data leaks, and the comparison of the implementation of personal data protection in the Indonesian banking sector with other countries in order to enrich the treasures of legal science and data protection policies.

**REFERENCES**

Antara News. (2013). Citibank is investigating the theft of customer credit card data. https://www.antaranews.com/berita/365435/citibank-selidiki-pencurian-data-kartu-kredit-nasabah

Balqis Fallahnda. (2023). Chronology of LockBit Suspected of Stealing BSI Customer Data & Latest Update Chronology of the alleged theft of BSI data carried out by Lockbit. tirto.id. https://tirto.id/kronologi-lockbit-diduga-curi-data-nasabah-bsi-update-terkini-gHpm

CNN Indonesia. (2022a). Leaked Immigration, Consumer Loans, and Bank Data for Sale on Raid Forum. https://www.cnnindonesia.com/teknologi/20220114143428-185-746695/data-imigrasi-konsumen-pinjol-dan-bank-bocor-dijual-raid-forum

CNN Indonesia. (2022b). Bank Indonesia Data Leak Has Not Been Completed, Rising to 74GB. https://www.cnnindonesia.com/teknologi/20220124163634-185-750569/kebocoran-data-bank-indonesia-belum-selesai-naik-jadi-74gb

CNN Indonesia. (2023). Error Since Monday, the President Director of BSI apologizes and guarantees that customer funds are safe. CNN Indonesia. https://www.cnnindonesia.com/ekonomi/20230510184413-78-947935/error-sejak-senin-dirut-bsi-minta-maaf-dan-jamin-dana-nasabah-aman

Hanif Reyhan Ghifari. (2023). BSI Records the Number of Customers Reaches 19.2 Million Until September 2023. https://tirto.id/bsi-catat-jumlah-nasabah-capai-192-juta-hingga-september-2023-gRJy

International Telecommunication Union. (2018). https://www.itu.int/pub/D-STR-GCI.01-2018

Jonathan Jordan Sianipar & Marta Solavide Naibaho. (2024). WEAK SECURITY OF GOVERNMENT BANKS IN INDONESIA: A CASE STUDY OF BRI BANK HACKING AGAINST ITS CUSTOMERS. 1(6). https://doi.org/10.61722/jmia.v1i6.2935

Lavinda. (2023). BSI Urged to Be Transparent About Alleged Customer Data Leaks. katadata.co.id. https://katadata.co.id/digital/teknologi/6465c013bf465/bsi-didesak-transparan-soal-dugaan-kebocoran-data-nasabah

Nikita Dewi Kurnia Salwa. (2024). Major Challenges & Obstacles Faced by CSIRT-BSSN Indonesia. https://csirt.or.id/pengetahuan-dasar/tantangan-csirt-bssn

Article 1 paragraph 5, Law of the Republic of Indonesia Number 27 of 2022. https://peraturan.bpk.go.id/Details/229798/uu-no-27-tahun-2022

Article 39 Paragraph 1, PDP Law No. 27 of 2022.

Article 46, Law of the Republic of Indonesia Number 27 of 2022.