JOURNAL OF LEGAL AND SOCIAL CHANGES
Scientia Plus Corp
P-ISSN: 00000
E-ISSN: 00000

Analysis of Personal Data Protection at Bank Syariah Indonesia Under Law No. 27 of 2022

Wildan Fattahur Rozaq 1[1*]

[1] Faculty of Law and Political Science, Muhammadiyah University of Surakarta, Sukoharjo, center Java, Indonesia, 57169
[*] c100210143@student.ums.ac.id

Article

Keywords:
Personal data protection; Bank Syariah Indonesia; Personal Data Protection; IT Security; Financial Services

Article History
Received: Apr 14, 2026;
Reviewed: Apr 16, 2026;
Accepted: Apr 29, 2026;
Published: May 1, 2026;

Abstract

Digital transformation has become BSI's priority in providing sharia-based financial services through digital technology. However, this transformation brings new challenges related to the protection of customers' personal data. This study aims to analyze the rights and obligations of personal data controllers with the implementation of BSI's obligations as a personal data controller based on Law Number 27 of 2022 concerning Personal Data Protection. Using an empirical legal method with a descriptive analysis approach, data was obtained from interviews with BSI and literature studies. The results of the study show data protection gaps at BSI in the form of the absence of leak notifications, lack of transparency in data disclosure to third parties, limited IT security responses, and inefficient data updates. This study recommends the development of data leak notifications, increased transparency, the formation of regional IT teams, and online services to update data.

INTRODUCTION

The rise of the digital age has driven the banking industry to develop financial services that leverage technological advancements to improve operational efficiency, streamline transaction processes, and provide better service to customers (Maulana & Apriani, 2021). However, these advancements also pose new risks, namely personal data breaches (Lutfi et al., 2024). In response to this, Law No. 27 of 2022 on Personal Data Protection has established obligations that must be fulfilled by every data controller (Fikri & Rusdiana, 2023). One such obligation applies to the banking sector in order to protect customers' personal information.

According to data from the Ministry of Communication and Information Technology, there was a significant surge in data breach cases from 2019 to 2023.

Figure 1 shows that between January and June 2023, there were 35 recorded data breach cases, exceeding the total number of cases that occurred during the 2019–2021 period. One notable incident was the case involving BSI in May 2023. Transaction disruptions on May 8, 2023, marked the beginning of this incident, during which the Russian hacker group Lockbit claimed to have successfully stolen 1.5 TB of customer data. The group subsequently demanded a ransom of Rp 296 billion. However, as negotiations failed, the data was ultimately leaked onto the dark web on May 16, 2023 (Data Protection for Beginners, 2023).

BSI, as the controller of personal data, bears full responsibility for managing and protecting its customers' data, regardless of whether or not there was any fault on the part of the bank or other relevant parties, in accordance with Law No. 27 of 2022 on Personal Data Protection (Hasna, 2023). This study aims to analyze the relationship between the rights and obligations of personal data controllers as stipulated in Law No. 27 of 2022 and the fulfillment of BSI's obligations as a personal data controller under said Law. Thus, the research questions posed are: (1) What are the rights and obligations of personal data controllers as stipulated in Law No. 27 of 2022 on Personal Data Protection? (2) Has BSI fulfilled its obligations as a personal data controller in accordance with Law No. 27 of 2022 on Personal Data Protection?

METHOD

This study employs an empirical legal approach using a descriptive-analytical research design to examine the implementation of BSI's obligations as a personal data controller under Law No. 27 of 2022. Primary data was obtained through interviews with BSI representatives, while secondary data included primary legal sources from Law No. 27 of 2022 and secondary sources such as books, journals, and BSI annual reports. Data collection was conducted through literature review and interviews, with descriptive-qualitative data analysis to evaluate the alignment of BSI's practices with legal provisions.

RESULTS AND DISCUSSION

Rights and Obligations of Personal Data Controllers Under Law No. 27 of 2022

A personal data controller refers to a public agency and/or individual who, independently or collectively, determines the purposes and controls the processing of personal data (Law No. 27 of 2022). Personal data protection encompasses various measures aimed at securing personal information during the processing process, to ensure the constitutional rights of data subjects (Rosadi & Pratama, 2018). A personal data controller is entitled to collect personal data for clear and legitimate purposes, and in accordance with the consent of the individual concerned. The obligations of a personal data controller are detailed in Articles 20 through 54 of Law No. 27 of 2022. Some of the main obligations include (Pakpahan, 2024):

1) The personal data controller must ensure that data processing has a legal basis, such as the data subject's consent, contractual or legal obligations, protection of vital interests, public duties, or other legitimate interests.

2) Personal data controllers must provide clear information to data subjects regarding the purpose, type of data, retention period, duration of processing, data subject rights, and policy changes.
3) Personal data controllers must process data in a limited, specific, transparent, and lawful manner.
4) Personal data controllers must process data in accordance with the previously established purpose.
5) The personal data controller must ensure data is accurate, complete, and consistent through verification.
6) The personal data controller must update/correct data within 3x24 hours of the data subject's request and confirm the results.
7) Data controllers must record all personal data processing activities.
8) Data controllers must provide access to data along with processing records in accordance with retention periods.
9) Data controllers must reject requests for changes if they endanger the security of the data subject or other individuals, disclose data belonging to third parties, or conflict with national security.
10) The personal data controller must conduct a data protection impact assessment if the processing involves high risk.
11) The personal data controller must protect data by implementing technical and operational measures, determining an appropriate security level based on the characteristics and risks of the personal data being processed, and preventing unauthorized access to personal data by implementing a reliable, secure, and responsible security system, whether in manual processing or through electronic systems.
12) The personal data controller must supervise involved third parties and ensure data protection against unlawful processing.
13) The personal data controller must cease processing if the data subject withdraws consent.
14) The personal data controller must suspend or restrict processing, either partially or entirely, upon the data subject's request and provide notification.
15) The data controller must cease, delete, or destroy data after the retention period ends, the purpose is achieved, upon the data subject's request, or in the event of unlawful processing.
16) The data controller must provide written notification to the data subject or relevant authority in the event of a data breach, including details of the leaked data, the time, the cause, and the corrective measures taken.

2. Analysis of the Implementation of Personal Data Controller Obligations by Bank BSI

As a personal data controller, BSI is required to comply with these provisions by implementing legal, security, and ethical measures in the management of customer data (Pakpahan, 2024). BSI has fulfilled its obligations as a personal data controller as follows:

1) Basic Legal Grounds for Processing Personal Data

According to BSI's privacy policy, the legal grounds for BSI's data processing include legitimate business interests, compliance with legal

obligations, fulfillment of contractual obligations with customers, and explicit customer consent (Bank Syariah Indonesia, 2024).

According to Mr. Brahim Wijaya, Branch Manager of BSI KCP Sukoharjo Kartasura, the legal basis for BSI's processing of personal data is grounded in circulars from the OJK and Bank Indonesia (Wijaya, 2024). Based on the policies, privacy statements, and explanations provided by Mr. Brahim Wijaya, it is evident that BSI has fulfilled its obligation to ensure that data processing is conducted on a legal basis. The application of this legal basis encompasses the fundamental principle of explicit customer consent, the fulfillment of legal obligations and agreements with customers, and is carried out in accordance with applicable regulations, as stipulated by the OJK and BI.

2) Purpose of Personal Data Processing

According to Mr. Brahim Wijaya, Branch Manager of BSI KCP Sukoharjo Kartasura, the collection of personal data by BSI serves as the basis for providing various services to customers (Wijaya, 2024). Additionally, based on BSI's policies and privacy guidelines, the purpose of the collected data is for the provision, development of products and services, as well as the execution of transactions such as investments and banking (Bank Syariah Indonesia, 2024). Based on BSI's policies and privacy guidelines, as well as Mr. Brahim Wijaya's explanation, it is evident that BSI has fulfilled its obligation requiring the data controller to process personal data in accordance with pre-established purposes. The fulfillment of this obligation is reflected in the data collection purposes, which serve as the basis for providing various services and supporting the development of products and services.

3) Obligation to Provide Information to Data Subjects According to BSI's policies and privacy statement, the data collected by

BSI includes information such as full name, gender, National ID Number (NIK) or other identification documents, place and date of birth, residential address, and Taxpayer Identification Number (NPWP), as well as other data (Bank Syariah Indonesia, 2024). According to Mr. Brahim Wijaya, Branch Manager of BSI KCP Sukoharjo Kartasura, the types of data collected by BSI are gathered in stages and tailored to the needs of the services provided. For example, when opening an account, customers are asked to provide personal data such as their NIK and KTP (Wijaya, 2024). Based on BSI's policies and privacy statement, as well as Mr. Brahim Wijaya's explanation, it is evident that BSI has fulfilled this obligation, particularly by providing clear information to data subjects regarding the types and relevance of the data to be processed. Additionally, the types of data collected including name, NIK, place and date of birth, address, and other data mentioned in the privacy policy reflect the obligation to provide detailed information about the data being collected.

4) Obligation to Ensure the Accuracy of Personal Data

According to Mr. Brahim Wijaya, Branch Manager of BSI KCP Sukoharjo Kartasura, BSI implements a customer data verification mechanism that ensures accuracy and consistency with data from the Population and Civil Registration Office (Disdukcapil). For example, if there is a change in the NIK,

BSI's internal data will be updated after being re-verified with official information from the customer (Wijaya, 2024). Based on Mr. Brahim Wijaya's explanation, it is evident that BSI has fulfilled its obligation to ensure data is accurate, complete, and consistent through verification. The fulfillment of this obligation is reflected in the verification of customer data against data from the Disdukcapil to ensure the data matches the actual information.

5) Obligation to Update Inaccuracies in Personal Data.

According to Mr. Brahim Wijaya, Branch Manager of BSI KCP Sukoharjo Kartasura, the process of changing data at BSI is carried out through a mechanism that requires customers to visit the Customer Service (CS) department in person. For example, when a customer wishes to change their NIK, BSI has a systematic procedure to update customer data precisely and accurately (Wijaya, 2024).

Based on Mr. Brahim Wijaya's explanation above, it is evident that BSI has fulfilled its obligation to update or correct data within 3x24 hours. The presence of a Customer Service (CS) team serving customers also reflects BSI's implementation of its obligation to provide data access along with processing records in accordance with retention periods. However, this approach also has weaknesses, such as the potential for limited access for customers who live far from a branch office or face time constraints.

6) Obligation to Record Every Related Activity Regarding the Processing of Personal Data.

According to Mr. Brahim Wijaya, Branch Manager of BSI KCP Sukoharjo Kartasura, BSI's recording system is directly connected to the Population and Civil Registration Agency (Dukcapil). For example, beyond face recognition technology, which is connected directly to Dukcapil data for customer identity verification (Wijaya, 2024).

Based on the statement from Mr. Brahim Wijaya, the BSI Branch Manager, this demonstrates that BSI, as the data controller, has fulfilled its obligation to record all personal data processing activities. The implementation of beyond face recognition technology integrated with Dukcapil reflects BSI's commitment to protecting customers' personal data, particularly in ensuring that the processed data has been accurately verified.

7) Obligations of the Personal Data Controller in Ensuring Security and Compliance with Regulations

In accordance with BSI's policies and privacy guidelines, customer personal data is shared with third parties solely for legal, service, collaboration, or marketing purposes. Third parties are required to maintain data security, limit its use to the intended purpose, and comply with customer consent, reflecting BSI's commitment to protecting privacy (Bank Syariah Indonesia, 2024).

According to Mr. Brahim Wijaya, Branch Manager of BSI KCP Sukoharjo Kartasura, the provision of access to personal data to third parties is primarily intended for the promotion of specific products. The personal data disclosed is limited to information such as the customer's name and workplace location (Wijaya, 2024). Based on the privacy policy and Mr. Brahim Wijaya's

explanation above, BSI has fulfilled its obligation to protect data through technical and operational measures. However, the explanation does not explicitly address the disclosure of data to third parties for marketing purposes or product offers, which are conducted with valid and explicit customer consent, potentially conflicting with this obligation. Furthermore, Mr. Brahim Wijaya, Branch Manager of BSI KCP Sukoharjo Kartasura, also explained that BSI has implemented a system for classifying customers' personal data based on security risk levels into three tiers: low, medium, and high, based on the customers' background and biographical profiles (Wijaya, 2024).

Based on Mr. Brahim Wijaya's explanation, it is evident that BSI has fulfilled its obligation to determine an appropriate security level commensurate with the characteristics and risks of the personal data being processed. By categorizing data into low, medium, and high risk levels, BSI can allocate security resources appropriately to protect more sensitive data. Furthermore, according to BSI's annual report, the bank has established the Chief Security Officer Office Group, which serves as the central hub for managing cybersecurity. The Chief Security Officer Office Group is responsible for safeguarding customer data confidentiality, protecting data from potential cyberattacks, and ensuring security systems operate optimally (Bank Syariah Indonesia, 2023).

Mr. Brahim Wijaya, Branch Manager of BSI KCP Sukoharjo Kartasura, also explained that BSI has a security system—the Chief Security Officer Office Group—which plays a crucial role in safeguarding overall data security (Wijaya, 2024). Based on Mr. Brahim Wijaya's explanation and the annual reports mentioned above, it is evident that BSI has fulfilled its obligation to prevent unauthorized access to personal data by implementing a reliable, secure, and responsible security system. The establishment of the Chief Security Officer Office Group reflects a strong commitment to protecting customers' personal data from potential cyber threats. Furthermore, Mr. Brahim Wijaya also explained that to enhance data security, BSI does not use general-purpose platforms like WhatsApp and Telegram but has adopted an internal application specifically designed for the company to share data (Wijaya, 2024).

However, the interview revealed that the implementation of IT security systems at the branch level remains limited to policies set by headquarters. Mr. Brahim Wijaya acknowledged that branches do not have the authority to directly manage IT security technical aspects (Wijaya, 2024). Based on Mr. Brahim Wijaya's explanation above, BSI's use of internal applications for various data also reflects that BSI has fulfilled its obligation to protect data through technical-operational measures. Furthermore, the use of internal applications reflects BSI's efforts to prevent unauthorized access to personal data by implementing a reliable, secure, and responsible security system. However, the limited authority of branches to manage the technical aspects of IT security indicates a complete reliance on headquarters to handle data security incidents.

8) Obligation to Monitor Third Parties

Mr. Brahim Wijaya, Branch Manager of BSI KCP Sukoharjo Kartasura, explained that BSI conducts daily monitoring of third parties granted access to personal data. Mr. Brahim Wijaya also emphasized that every day, BSI requests updates regarding the results of such data usage to ensure that the data is used solely for the purposes of the collaboration (Wijaya, 2024). Based on Mr. Brahim Wijaya's statement, it is evident that BSI has fulfilled its obligation to monitor involved third parties and ensure data protection against illegal processing. By requesting daily updates on data usage results, BSI not only maintains control over data processing but also reduces the risk of data misuse or leakage.

9) Obligation to Cease Processing of Personal Data

According to BSI's policies and privacy guidelines, customers' personal data will be retained by BSI as long as the customer continues to use the services or in accordance with applicable banking laws and regulations, and will be destroyed upon the expiration of the retention period (Bank Syariah Indonesia, 2024). Based on the aforementioned BSI policies and privacy guidelines, it is evident that BSI has fulfilled its obligation to cease, delete, or destroy data upon the expiration of the retention period, the achievement of the intended purpose, a request from the data subject, or in cases of unlawful processing. This measure also reflects BSI's commitment to preventing potential data misuse once the data is no longer relevant through secure destruction procedures after it is no longer required.

10) Obligation to Provide Notification in the Event of a Personal Data Breach

Based on an interview with Mr. Brahim Wijaya, Branch Manager of BSI KCP Sukoharjo Kartasura, BSI does not yet have a dedicated notification system to inform customers about data breach incidents. To date, notifications provided to customers have been limited to financial transactions such as cash withdrawals, transfers, or deposits via the SMS notification system (Wijaya, 2024).

Mr. Brahim Wijaya's explanation indicates that BSI has not fulfilled its obligation to provide written notification to relevant individuals or institutions in the event of a data breach, including details of the leaked data, the time, the cause, and the response measures. Reliance on the central system without an emergency response mechanism at the branch level highlights potential gaps in coordination and response to data security incidents.

As a data controller, BSI has endeavored to fulfill most of its obligations as a controller of personal data under Law No. 27 of 2022. However, there are still several obligations that have not been fully implemented or fulfilled by BSI.

No.	Weaknesses	Data Source	Solutions
1	There is no specific notification system for data breaches	Interview with Mr. Brahim Wijaya as Branch Manager of BSI KCP Sukoharjo	Develop an automated notification system and conduct emergency response training across all branches

2	Use of customer data by third parties without valid and explicit consent from the data subject	BSI Privacy Policy and interview with Mr. Brahim Wijaya as Branch Manager of BSI KCP Sukoharjo	Ensure explicit consent from customers before their data is used for marketing or product offerings
3	Slow response to security incidents due to centralized IT management at headquarters	Interview with Mr. Brahim Wijaya as Branch Manager of BSI KCP Sukoharjo	Establish regional IT teams to handle incidents at the branch level more quickly
4	The data update process requires customers to visit the branch in person	Interview with Mr. Brahim Wijaya as Branch Manager of BSI KCP Sukoharjo	Provide online services through digital applications to facilitate customer data updates without visiting the branch

First, BSI does not yet have a dedicated notification system to inform customers in the event of a personal data breach. To address this, BSI needs to develop a notification system to alert customers in the event of a personal data breach, accompanied by an explanation of the steps taken to address the incident.

Second, BSI has not ensured that the disclosure of personal data to third parties, particularly for marketing or product offers, is conducted with the valid and explicit consent of the data subject. To address this, BSI must ensure transparency regarding third-party use of data for marketing or product offers by obtaining explicit consent from consumers before the data is used, in accordance with personal data protection principles.

Third, BSI's IT security management, which remains centralized at the headquarters, limits branches' ability to respond to security incidents promptly. To address this, BSI should consider establishing regional IT teams so that branches are not overly reliant on the headquarters when handling security issues.

Fourth, the data update process, which requires customers to visit a branch in person, poses difficulties for those in remote locations or with time constraints. To address this, BSI needs to provide online services or digital applications that allow customers to update their data without having to visit a branch in person, making it more convenient for customers in remote areas or those with limited time.

CONCLUSION

Based on the analysis conducted of the research findings and discussion, the following conclusion can be drawn: the data controller has the right to collect personal data for clear and legitimate purposes, and based on the data subject's consent. Additionally, the personal data controller is obligated to ensure a legal basis for data processing, provide information to the data subject, process data lawfully and transparently, process data in accordance with the purpose, ensure data accuracy, update data within 3x24 hours, record processing activities, grant data subjects access rights, reject unlawful modifications, assess data protection risks, protect personal data, supervise relevant parties, cease processing if consent is withdrawn, suspend processing upon request, destroy data after the retention period ends, and provide written notification of data protection breaches.

BSI has not fully fulfilled its obligations as a personal data controller, which include the absence of a notification system for personal data protection failures, data disclosure for marketing or product offers not being based on explicit customer consent, IT security systems at the branch level being limited and dependent on the central office, and data update mechanisms through Customer Service being ineffective for customers with limited access.

REFERENCES

UNDANG-UNDANG

Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi, Jakarta: Lembaran Negara Republik Indonesia, Tahun 2022 Nomor 196

PENERBITAN PEMERINTAH ATAU LEMBAGA LAINYA

Laporan Tahunan 2023 PT Bank Syariah Indonesia, Tbk, Jakarta: Bank Syariah Indonesia.

JURNAL

Maulana, R. A., & Apriani, R. (2021). *Perlindungan Yuridis Terhadap Data Pribadi Nasabah Dalam Penggunaan Elektronik Banking (E-Banking). 7*(2).

Lutfi, M. P., Kurniasari, E., & Putri, F. E. A. (2024). Urgensi Perlindungan Hukum Terhadap Data Privasi Nasabah Bank Di Era Perkembangan Digital. *Jurnal Multidisiplin Ilmu Akademik*, 1(5), 210-218.

Fikri, M., & Rusdiana, S. (2023). Ruang Lingkup Perlindungan Data Pribadi: *Kajian Hukum Posistif Indonesia. Ganesha Law Review*, 5(1), 39-57.

Rosadi, S. D., & Pratama, G. G. (2018). Perlindungan privasi dan data pribadi dalam

era ekonomi digital di Indonesia. *VeJ*, 4(1), 88-110.

Pakpahan, JM (2024). Kesadaran Urgensi Peran Pengendalian dan Pemrosesan Data Pribadi dalam Rangka Pelindungan Data Pribadi Individu Berdasarkan Undang-Undang Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi. *Jurnal Hukum to-ra: Hukum Untuk Pengaturan dan Melindungi Masyarakat* , 10 (1), 119-137.

SKRIPSI

Hasna, K. (2023). *Kendala Implementasi Perlindungan Hukum Keamanan Data Pribadi Nasabah Bank BSI Atas Ancaman Ransomware* (Doctoral dissertation, Universitas Islam Indonesia).

INTERNET

METRO TV. (2023, July 19). *Rangkuman Kasus Kebocoran Data di Indonesia* [Video]. YouTube. https://www.youtube.com/watch?v=MQ0S2Puyqro

Bank Syariah Indonesia, "Kebijakan Privasi BSI" dalam *Bank Syariah Indonesia*, https://www.bankbsi.co.id/kebijakan-privacy/bsi