Analysis of Legal Protection for Consumer Personal Data and the Responsibilities of Banks

Dyah Ersita Yustanti

[1] Universitas 17 Agustus 1945 Jakarta, Jakarta, Indonesia
dyustanti@yahoo.com

Abstract. Protection of personal data has become an urgent issue with the advent of digital technology in the era of Big Data. Concerns about privacy and unauthorized use of data are growing as governments and private companies collect large amounts of data. The banking sector, which stores sensitive personal information, is vulnerable to risks such as unauthorized sale of customer data and data leakage, as happened to Bank Syariah Indonesia (BSI). In this study, normative juridical research methods are used by reviewing primary and secondary legal materials to answer problem formulations related to the legal protection of consumers for personal data and the Bank's responsibility for consumer personal data. This research is important to maintain a balance between technological innovation and personal privacy and provide guidance for legislators and relevant institutions in regulating and protecting personal data. The form of protection of customer data shows that Bank Indonesia Regulation Number 7/6/PBI/2005 concerning Transparency of Bank Product Information and Use of Customer Personal Data is the main foundation in this regard. The bank's responsibility for losses suffered by customers is internal and external. This means that the bank has responsibility for the actions of its employees who leak data. However, banks are also responsible for customers who suffer losses as a result of such actions. Banking sector has strong personal data protection due to regulations and standardization, but still needs additional authority to oversee data quality.

Keywords: Corporate and Commercial Law, Legal protection, Personal data.

1 Introduction

The development of digital technology has raised increasingly urgent issues related to personal data protection. In the era of Big Data, where data is collected in large and untold amounts by governments and private companies, concerns about privacy and unauthorized use of data are increasing. Data collected in Big Data includes Personal Data, which is any data about a person's life either identified and/or identifiable separately or combined with

A. A. Nassihudin et al. (eds.), *Proceedings of the 3rd International Conference on Law, Governance, and Social Justice (ICoLGaS 2023)*, Advances in Social Science, Education and Humanities Research 805,
https://doi.org/10.2991/978-2-38476-164-7_114

other information either directly or indirectly through electronic and/or non-electronic systems.[1] [2]

One sector with access to susceptible personal data is the banking sector, where customers' data is stored and must be kept confidential. In general, Personal Data Protection in Electronic Systems includes protection against the acquisition, collection, processing, analysis, storage, display, announcement, transmission, dissemination, and destruction of Personal Data. protected by Law Number 27 of 2022 concerning Personal data protection, which is the obligation of the personal data controller. In particular, banks must maintain customer data, following Article 1 number 28 of Law Number 7 of 1992 concerning Banking as amended by Law Number 10 of 1998 concerning Amendments to Law Number 7 of 1992 concerning Banking, explaining that bank secrets are everything related to information about depositors and their deposits.

The principle of bank secrecy not only aims to protect the interests of bank customers to be protected by confidentiality regarding financial conditions and customer personal data, in addition, bank secrecy is also intended for the interests of the bank itself because the bank will be trusted by customers to manage their finances One clear example that reflects this anxiety is the existence of a crime mode of buying and selling personal data to investment or insurance companies, So often consumers are contacted and offered by companies that sometimes have nothing to do with the bank they use.[2]

In the digital era, data leakage cases are also a frequent threat, one of which is the recent BSI bank customer data leak case. Known, group ransomware LockBit 3.0 claims to have disseminated customer data in the Dark Web after several requests for money requested were not fulfilled by BSI. About 80 percent of customer data is alleged to have been stolen when the group paralyzed BSI Bank's Information Technology (IT) system for three days. This hack is a type of cyber attack commonly called[3] ransomware. Hackers encrypt valuable data belonging to the target and then ask for a sum of money to unlock it. This incident raises great concerns about the vulnerability of bank customers' personal data which should be closely guarded.

Therefore, personal data protection has become a crucial topic in law, which requires strong legislation to protect individual rights and maintain a balance between technological innovation and personal privacy. Cases such as the BSI bank customer data leak show the need for strict regulations in managing and protecting personal data, especially in the financial sector which has access to highly sensitive information.

2 Problems

Based on the above opening, the problems in this journal are:

a. What are the regulations regarding the protection of customers' personal data according to applicable laws?

b. What is the Bank's responsibility for consumers' personal data?

3 Method

This study used normative juridical research methods. Normative juridical research is legal literature research conducted by reviewing primary and secondary legal materials using a statutory approach and an analysis approach to legal concepts, which is carried out by reviewing all laws and regulations related to legal issues.[4] Normative legal research serves to provide juridical argumentation when there are gaps, vagueness, and conflicts of norms. Furthermore, legal research has a role in maintaining the critical aspects of legal science as a normative science that *sui generis*. [7]

4 Discussion

4.1 Regulation on the Security of Personal Data of Bank Customers

States must protect, promote welfare, educate, and participate in implementing world order. In an increasingly advanced digital era, the development of information technology brings significant new challenges, especially in terms of digital security and personal data protection. In this context, the importance of personal data security becomes very relevant, especially in the use of electronic systems such as *e-banking* services and banking websites. When customers register with the bank, they are required to enter their personal data, and this data should be considered a company secret that must be protected. Therefore, banks have a great responsibility in safeguarding and protecting the personal data of their customers.

In the banking sector, Bank Indonesia has a role given the authority and obligation to foster and supervise banks. Bank Indonesia carries out this task by taking a preventive approach. In the Banking Law, it is explained that in terms of utilizing information technology, the Bank has provisions governing the implementation of electronic systems and transactions, as well as the protection of personal data. These provisions include the obligation to apply the principles of personal data protection when processing data, obtain valid consent from the owner of personal data for certain purposes involving the Customer and/or Consumer, carry out risk management, delete or stop the use of personal data and transaction processing if the Customer and/or Consumer revokes the consent given, and implement appropriate governance policies and procedures. [5]

The Electronic Information and Transaction Law indirectly governs electronic data protection for both public and private purposes but lacks clarity on safeguarding personal information. It defines the protection of electronic systems against unauthorized usage, ensuring operator security, and preventing unlawful access. An electronic system encompasses electronic devices and processes for information handling. Personal data in

electronic media requires owner consent, with legal repercussions for violators. Unauthorized personal information use through electronic means infringes on privacy rights, creating uncertainty for data custodians and government bodies.

President Jokowi signed Law Number 27 of 2022 on October 17, 2022, establishing robust Personal Data Protection, a significant step in safeguarding individual data. The law prioritizes data protection while upholding constitutional rights, ensuring transparency in data usage. Article 5 empowers data subjects with insights into requestor identity, legal basis, motives, and responsibilities. Article 13 allows data subjects to access and use their data in standard formats, acknowledging the digital age's data portability. They also have the right to transmit their personal data to other personal data controllers, provided that the systems used can communicate securely following personal data protection principles.[6] Article 16 sets the rules for processing personal data, including acquisition, processing, storage, correction, updating, display, announcement, transfer, dissemination, disclosure, and deletion. Processing must be legal, transparent, and secure. Personal data must be accurate, complete, up-to-date, and accountable. Article 21 requires the controller to provide information about the data subject's rights. Article 34 calls for an impact assessment of high-risk data. Article 56 permits data transfer outside of Indonesia without considering the data owner's rights, which contradicts the law's objective of improving personal data protection.

The Financial Services Authority of the Republic of Indonesia has issued Regulation Number 11/POJK.03/2022 to oversee information technology usage in commercial banks. This grants them authority over IT and cyberbanking security and mandates robust IT governance. Banks must define authorities and responsibilities across all levels, establish policies, standards, and procedures for effective IT use, and create an IT implementing unit. Adherence to this regulation is vital for banks to avoid administrative penalties, and they must prioritize confidentiality, integrity, and availability principles. This requires a strong risk management information system encompassing factors like human resources, processes, technology, and environment, as well as internal controls and IT audits per the Financial Services Authority's guidelines.

In addition, it is essential for banks to have a disaster recovery plan in place to maintain operations during natural disasters or IT disruptions. Regular testing and reviews of this plan are crucial to its effectiveness. Given the increasing threat of cyberattacks like ransomware, banks must enhance their cybersecurity resilience. Periodic cybersecurity testing is one measure to secure networks, systems, and data. The Financial Services Authority of the Republic of Indonesia has categorized cybersecurity testing into two primary types: vulnerability analysis-based testing and scenario-based testing under Regulation Number 29/SEOJK.03/2022.

Vulnerability analysis-based cybersecurity testing is essential for identifying weaknesses in a bank's systems. Evaluation frequency is determined by internal

assessments, considering factors like system criticality and cybersecurity exposure levels. The process involves pinpointing vulnerabilities and conducting thorough penetration testing on hardware and software used by the financial institution, particularly those related to digital operations and services.

Conversely, scenario-based cybersecurity testing is crucial for verifying a bank's incident response and recovery protocols and the effectiveness of its communication strategy in handling cybersecurity risks. A comprehensive testing approach involves engaging various stakeholders, including executive officers, business units, corporate communications teams, crisis management personnel, service providers, and technical staff responsible for incident detection, response, and recovery processes.

Scenario-based cybersecurity tests encompass tabletop exercises, cyber range exercises, social engineering exercises, and adversarial attack simulation exercises. Table-top exercises bring key personnel together to discuss and plan emergency response under the guidance of a skilled facilitator. Cyber range exercises use simulated representations of the bank's networks and systems for controlled testing, allowing for assessment without operational disruptions. Social engineering exercises evaluate employee cybersecurity awareness by simulating scenarios where attackers attempt to trick employees into revealing sensitive information. The Adversarial Attack Simulation Exercise (AASE) involves a realistic cyber-attack simulation, testing the bank's ability to prevent, detect, and mitigate cyber threats with red team (attackers) and blue-team (defenders) interactions.

Simulation-based testing requires close supervision to prevent system disruptions. Threat scenarios should be based on potential cybersecurity threats, enabling banks to proactively search for threats and leverage relevant threat intelligence to identify potential threat actors and tactics. Banks are mandated to conduct cybersecurity tests annually, reporting their research results to the Financial Services Authority within 10 working days. To meet this requirement, banks should establish an independent unit or function responsible for their cybersecurity and resilience. While banks can engage third-party IT service providers in their IT operations, they are still required to have the capacity to oversee the activities carried out by the bank. As a result, there is a need for policies and procedures that encompass, at a minimum:

a. The process of identifying the need for third-party IT service usage;
b. The process of selecting third-party IT service providers;
c. Guidelines for establishing working relationships with third-party IT service providers;
d. Risk management procedures for using third-party IT service providers; and

e. Methods for assessing the performance and compliance of third-party IT service providers.

The IT service provider must possess the necessary qualifications, competencies, and human resources. When a bank partners with an IT service provider, a clear understanding of working principles and a formal cooperation agreement must be established. Cost-benefit analysis, risk management, and a tested Disaster Recovery Plan must be in place to ensure caution is upheld. Additionally, mechanisms for reporting, handling critical incidents, and other responsibilities must be agreed upon.

The bank must promptly inform the Financial Services Authority within three working days of any IT service provider performance issues that could impact the bank's operations. This includes breaches of confidentiality or customer data regulations, IT service provider insolvency, legal action, and other conditions disrupting or terminating IT service provision. The bank must decide on appropriate follow-up actions, potentially terminating the IT service provider's use, and report to the Financial Services Authority within three working days if needed.

Structured and periodic cybersecurity testing is a critical tool for banks to identify and address cybersecurity risks, ensuring preparedness for potential incidents. Successful cybersecurity testing helps banks mitigate risks, maintain public trust, and ensure operational continuity.

In Indonesia, personal data protection regulations are fragmented, lacking a comprehensive framework. In contrast, European Union (EU) law, through the General Data Protection Regulation (GDPR), defines personal data broadly and mandates strict protection. Each EU member state has its own Data Protection Agency (DPA) to oversee GDPR implementation and handle complaints. The GDPR covers a wide range of personal information, prohibiting disclosure without explicit consent, except in emergencies or law enforcement cases.[7]

On the other hand, Indonesia's Law No. 27 of 2022 mirrors some regulations, including penalties, but lacks an independent supervisory institution, unlike the GDPR's stringent requirements for data protection agencies. An independent supervisory body is crucial to prevent conflicts of interest and ensure effective protection, meeting the "adequate level of protection" standard. In the EU, personal data protection policies are stricter, emphasizing individual protection and strong supervision by those with expertise in the digital field.

Malaysia and Indonesia share the goal of safeguarding personal data but differ in legal framework and enforcement. Malaysia has the PDPA Malaysia (Personal Data Protection Act No. 709 of 2010), covering all data types, with a dedicated enforcement department. Indonesia's Law No. 27 of 2022 has a broader scope but lacks a specific data

protection authority as of September 2021. Both countries recognize data subject rights, but regulations and enforcement may change, so consult local sources for updates.

In addition, South Korea's robust legal framework, the 2011 Personal Information Protection Act (PIPA), safeguards personal data for its large internet user population. PIPA enforces strict rules, earning global recognition for privacy protection.

While personal data protection laws are sufficient in theory, their success depends on practical implementation, compliance, and management. Therefore, Indonesia has the potential to enhance its data protection framework by considering technological advancements and privacy dynamics. Raising awareness and providing education on personal data protection are essential in preserving individuals' rights in the ever-changing digital age.

4.2 Bank's Responsibility for Personal Data

A bank, operating as a business entity, necessitates financial resources to facilitate its operational endeavors. These resources can be acquired through diverse channels. The origins of these financial resources available to the bank include its proprietary capital, derived from deposits made by bank proprietors or the issuance and trade of bank shares to potential new stakeholders. Alternatively, the bank can also access funds from external sources, such as borrowing from the general public or other financial establishments. Among these avenues, a primary and pivotal source of funds stems from the broader community, signifying a cornerstone for the bank's financial inflow. These community funds are an important source of funds for banking operations which is an indicator of the bank’s success if it has been able to finance its operations from these funds.[8]

Banks engage in a variety of activities to secure funding from the public, in accordance with Article 6 of Law Number 7 of 1992 concerning Banking, as amended by Law Number 10 of 1998. Commercial banks, in particular, are mandated by this law to accumulate funds from the general populace through various channels like current accounts, time deposits, certificates of deposit, savings accounts, and similar financial instruments. This fund aggregation is a fundamental aspect of a bank's operations and plays a pivotal role in their financial management. As highlighted by Muhammad Djumhana, the funds collected from the community are central to a bank's financial resources and are strategically employed to generate profitability. Safeguarding and growing these funds represent a critical function within the realm of banking, aligning with the principles outlined in Article 3 of the Banking Law. In essence, banks function as intermediaries in the financial sector, entrusted with the responsibility of gathering and distributing communal funds, underscoring their essential role as key players in financial intermediation. There are various types of fund storage offered by banks to the public to collect funds from the public, including:[9]

a. Current Deposit or Current Account

A current account, as defined in Article 1, number 6 of Law Number 10 of 1998 amending Law Number 7 of 1992 concerning Banking, is a deposit account that allows withdrawals through checks, payment orders, or bookkeeping, providing a flexible means of payment for various transactions.

b. Deposit

A deposit is a deposit whose withdrawal can only be made at a certain time based on the depositor's agreement with the bank. Deposits can also be used as credit collateral.

c. Deposit Certificate

Is a deposit in the form of a deposit whose proof of storage certificate is transferable. A certificate of deposit is a security issued by appointment without the buyer's name in rupiah, which is an acknowledgment of debt from the bank and can be traded in the money market.

d. Savings

Savings are deposits whose withdrawals can only be made according to certain agreed conditions, but cannot be withdrawn by cheque, billet giro, and or other instruments likened to it

The collection and distribution of any funds offered by banks to the public should have a legal relationship that accompanies the banking service product. The legal law between customers and banks is divided into contractual relationships and non-contractual relationships. The contractual relationship between the banks and the customers regulates the rights and obligations of banks and customers, as well as dispute resolution mechanisms in the event of rising dispute, and also collection activities through current accounts, time deposits, certificates of deposit, savings, and or other forms likened to it which are based on fund storage agreements between the banks and the customers. Concerning bank obligations, as quoted by Sentosa Sembiring among them are:[10]

a. guarantee the confidentiality of the customer's identity along with the funds deposited with the bank, unless the laws and regulations specify otherwise;
b. Handing over funds to customers following the agreed agreement;
c. Pay interest on deposits according to the agreement;
d. Replace the position of the debtor if the customer is unable to carry out its obligations to third parties;
e. Make payments to exporters in the event of use of L/C facilities, provided that the requirements for it have been met;

f. Provide reports to customers on the development of their deposits in the bank; and

g. Return collateral if the credit has been paid off.

Furthermore, It's crucial to recognize the strong, unspoken connection between a bank and its customers, which goes beyond formal contracts. This underlying bond is based on trust, responsible behavior, and the protection of sensitive data, even though it's not explicitly outlined in any agreement. These intangible aspects define the core of the relationship.

Fund storage agreements form the basis of the legal relationship between banks and customers in fundraising activities through depository services. Legal relationships between customer banks often include arrangements distributed across multiple documents or forms, which can generally consist of the following four groups of documents or forms:[11]

a. Customer identification form (consumer identification file);

b. Fund field form (collection of public fund deposits);

c. Form in the field of credit (distribution back to the community); and

d. Form in the field of banking services.

Banks must safeguard personal data in fundraising forms. These forms tailor agreements between banks and depositors. Opening an account involves regulations governing application details, account terms, product specs, and legal guidelines. The complex framework underscores the need for banks to be diligent in preventing data breaches.

Further provisions in account opening are regulated in the General Terms of Account Opening (GTAO). GTAO is a master regulation relating to the bank's function as a fund collector that contains generally accepted provisions in every banking transaction. The functions of GTAO in the legal relationship between banks and customers, among others, are as follows:[11]

a. Regulate the rights and obligations of the parties, namely between the bank and the customer which is generally applicable to all accounts;

b. Clarify the applicability of the provisions or the submission of related provisions; and

c. As an educative effort for the bank to customers, by reinforcing several applicable laws and regulations that are considered important.

In the deposit product form at the bank, the customer's identity is contained as a condition that must be submitted by prospective customers to the bank before the form is signed. Filling in information data of prospective individual customers determined by the bank at least contains information about:[12]

a. Name, place, and date of birth, address, and nationality as evidenced by an ID card, driver's license, or passport and equipped with information about the permanent residence address if it is different from what is stated in the document. Especially for foreign nationals other than passports, proven by a Temporary Stay Permit Card (KIMS/KITAS) or Permanent Stay Permit Card (KITAP);

b. Address and telephone number of the working company equipped with information about the business activities of the company/agency where they work;

c. Information about the job/position and income of prospective customers. In case the nasal candidate does not have a job then the required data is the source of income;

d. Information about the source and purpose of using funds; and

e. Signature specimens.

According to the general provisions of the Financial Services Authority Circular Letter Number 14 / SEOJK.07 / 2014 concerning Confidentiality and Security of Consumer Data and/or Personal Information, personal data of individuals includes:

a. name;

b. address;

c. date of birth and/or age;

d. telephone number, and/or

e. birth mother's name.

Financial service entities, like banks, are prohibited from sharing a customer's personal information with external parties without the customer's consent. This rule is based on the concept of bank secrets outlined in Article 40 of Law Number 10 of 1998 regarding Banking. However, there are specific situations where this confidentiality can be breached:

a. For Tax Purposes: Bank secrets can be disclosed for tax-related reasons. Article 41 paragraph (2) of the Banking Law allows bank secrets to be revealed upon a written request from Bank Indonesia, initiated by the Minister;

b. For Settlement of Bank Debts: Article 41A of the Banking Law empowers the head of Bank Indonesia to grant permission to the State Receivables and Auction Affairs Agency/State Receivables Affairs Committee to access information about debtor customer deposits at the bank;

c. For Legal Proceedings: The head of Bank Indonesia may permit the police, prosecutor, or judge to access a customer's deposit information for criminal or civil

legal matters. This requires a written request from the Chief of Police of the Republic of Indonesia, the Attorney General, or the Chief Justice of the Supreme Court. These provisions are covered in Article 42 for criminal cases and Article 43 for civil cases;

d. Exchange Requirements for Interbank Information: Article 44 paragraph (1) of the Banking Law allows the exchange of information between banks to facilitate and secure their business activities, such as preventing duplicate credit and understanding the condition and status of other banks; and

e. With Customer Consent: Upon the request for approval or power of attorney from the depository customer or their heirs, as governed by Article 44A of Law Number 10 of 1998, amending Law Number 7 of 1992 concerning Banking.

As previously elucidated, the sanctity of bank secrets encompasses all facets of data of depositor clients and their entrusted funds. The individual's identity stands as a realm intricately linked to the depositor, constituting an integral component of the bank's confidential information. The bank and its affiliated entities have a responsibility to safeguard this information, except when legal provisions require disclosure. Affiliated parties encompass:

a. Board members, supervisors, directors, officers, and employees of the bank;

b. Management, supervisors, managers, officers, and employees of cooperative banks adhering to applicable laws;

c. Service providers to the bank, such as public accountants, appraisers, legal consultants, and other advisors; and

d. Entities assessed by Bank Indonesia as influencing the bank's management, including shareholders and their immediate families, as well as the families of commissioners, supervisors, directors, and management.[8]

The unauthorized dissemination of customer data through a web of online data vendors, often implicating bank personnel, particularly those involved in bank marketing, represents a blatant breach of banking confidentiality. These employees fall within the category of associated parties mandated to uphold the tenets of banking secrecy. The unauthorized trade in personal customer data exposes private information to the general public, opening the door for unscrupulous entities to exploit it for their benefit. Only upon receiving explicit consent from the affected customer can the obligations of banking secrecy be lifted, thereby nullifying the premise for maintaining such confidentiality.

Bank employees passing on customer's personal information to unauthorized parties without the customer’s permission is a violation of banking confidentiality. In legal science, the concept of legal responsibility recognizes that a person is said to be legally responsible for a particular act, is that he can be subject to a punishment in the case of the

opposite act.[11] Bank employees are responsible for keeping customer's personal information confidential. Leaking such information is considered negligence of the bank's secrecy provisions and can result in criminal charges. Violating bank secrets can lead to imprisonment for a minimum of 2 years and a fine of at least Rp4.000.000.000,00.

Personal data becomes part of the depositor and his deposit, which is included in a form agreed between the customer and the bank. The retention agreement forms the basis of the contractual relationship in which the parties have rights and obligations. Generally, the bank product form for opening an account does not explicitly state the bank's obligation to keep the customer's personal information confidential. Banking practices indicate that the obligation to maintain the confidentiality of its customer's information is not enshrined in the bank's deposit contract, but is generally contained in the company's rules on bank employees' obligations to the confidentiality of the financial status of customers shall be maintained as ordered by Law Number 7 of 1992 concerning Banking as amended by Law Number 10 of 1998.[12]

Banks are obligated to safeguard customer data, in line with industry standards and ethics, crucial for upholding customer trust and complying with the depository agreement. The Banking Law, Article 40, Paragraph (1) of Law Number 10 of 1998, designates customer data as a bank secret, mandating strict confidentiality, with exceptions detailed in subsequent articles.

Regarding breaches of customer data confidentiality by bank employees, responsibility does not fall solely on them. Banks share accountability due to the breach of bank secrecy regulations, stemming from the legal relationship between the bank and the customer, who possess rights and obligations under the Banking Law.

As key players in the financial sector, banks must prioritize consumer protection, as mandated by the Financial Services Authority Regulation Number: 1/POJK.07/2013 and Bank Indonesia Regulation Number: 16/1/PBI/2014. These regulations stress the importance of safeguarding consumer data.

The Financial Services Authority Regulation, Article 29, imposes strict accountability on banks for consumer losses, extending to mistakes, negligence, or actions by the banks, employees, or third parties. Banks bear responsibility for their employees' actions, leading to customer harm, including personal information exposure, confidentiality breaches, or financial losses.

Banks' civil liability for employee errors or negligence can be considered as management or corporate liability, as evidenced by precedent cases. The absence of specific instructions from bank management beyond designated powers and responsibilities reinforces the bank's overall responsibility, requiring them to cover losses from employee faults, in accordance with Article 1365 of the Civil Code, aligning with the principle that disadvantages are inherent to business operations.[13]

To address system errors or data breaches, banks must adhere to the Financial Services Authority of the Republic of Indonesia Regulation No. 11/Pojk.03/2022, which mandates the implementation of security protocols within their IT Risk Management framework. Additionally, banks are required to maintain a high level of cyber resilience, referencing key regulations like Government Regulation No. 71 of 2019 on Electronic Systems and Transactions, and Ministry of Communication and Informatics Regulation No. 20 of 2016 on Personal Data Protection in Electronic Systems

In the event of a failure in data protection, data controllers are obliged to take a series of actions in compliance with multiple regulations. First, banks must provide notifications to data subjects and the public in line with Article 46 of Law No. 27/2022. [14] This notification must be made within the specified timeframe, following the provisions of the Ministry of Communication and Informatics Regulation No. 20 of 2016. Furthermore, the Financial Services Authority Regulation requires the issuance of an initial notification within a shorter timeframe and the reporting of information technology incidents to the Financial Services Authority within a defined period after the incident.

Second, banks are required to implement disaster recovery plans following the applicable regulations to ensure operational continuity during incidents. The regulations also necessitate the alignment of incident response and recovery plans with business continuity plans, disaster recovery plans, crisis management plans, and other relevant bank policies.

Moreover, considering the sensitivity of personal financial data as a specific category of personal data, a higher level of protection is required. Therefore, specific measures are deemed necessary in handling data protection failures.

Third, the Financial Services Authority is responsible for evaluating mitigation measures and ensuring the updating of bank disaster recovery plans in compliance with regulations. A comprehensive audit and evaluation of information technology incident mitigation and recovery plans within the banking sector are also within the remit of the Financial Services Authority.

Fourth, the Ministry of Communication and Informatics (Kominfo), with its supervisory authority, must promptly investigate and resolve incidents accountably. This encompasses identifying the causes of personal data protection failures, determining the losses incurred by data controllers, processors, and data subjects, and announcing the results of the investigation and the actions taken. Furthermore, Kominfo must ensure the restoration of data subjects' rights.

Fifth, the National Cyber and Crypto Agency (NCCA) is responsible for monitoring and investigating cybersecurity incidents experienced by banks. NCCA will identify sources of attacks, pinpoint security vulnerabilities that enabled attacks and design necessary follow-up measures. Periodic security audits and the implementation of

strong security standards across the banking and financial sector are also central to NCCA's role.

5 Conclusion

Efforts that can be taken by customers who feel affected by information leakage are to file a complaint with the relevant bank. If this complaint does not produce a satisfactory solution, the customer has an alternative to request mediation from the banking institution. If the mediation does not result in an agreement between the bank and the customer, the customer still has the right to take the case to the District Court or the Consumer Dispute Settlement Agency (BPSK). The Bank Indonesia regulation provides a clear framework to protect customers' personal data and affirms the bank's responsibility to maintain the confidentiality of such information. Customers who feel aggrieved have legal channels and procedures that can be followed to seek justice and restoration of their rights. In its application, personal data protection in the banking sector is superior due to the existence of practical regulations and the development of standardization to maintain personal data security. However, apart from the Financial Services Authority, there should be a designated authority to handle and monitor the quality of personal data protection.

REFERENCES

[1] W. Djafar, "'Hukum perlindungan data Pribadi di Indonesia: Lanskap, Urgensi, dan Kebutuhan Pembaruan,'" 2019.

[2] V. Katiandagho, D. D. Putong, and I. J. Melo, "Undang – Undang Perlindungan Data Pribadi Memperkuat Undang – Undang Perbankan Dalam Menjaga Rahasia Data Nasabah Dan Untuk Melindungi Data Pribadi Masyarakat Indonesia," *J. Huk. to-ra Huk. Untuk Mengatur dan Melindungi Masy.*, vol. Vol. 9, no. No. 1, p. 106, 2023.

[3] Liputan6, "'Kelompok Ransomware LockBit Akhirnya Sebar 1,5 TB Data Karyawan dan Nasabah BSI ke Internet.'"

[4] Soekanto, *Penelitian Hukum Normatif (Suatu Kajian Singkat)*. Bandung: Rafika Aditama.

[5] Z. Aidi, "Implementasi E-Court Dalam Mewujudkan Penyelesaian Perkara Perdata Yang Efektif Dan Efisien," *Masal. Huk.*, vol. 49, no. 1, p. 80, 2020, doi: 10.14710/mmh.49.1.2020.80-89.

[6] B. A. Riswandi, *Aspek Hukum Internet Banking*. Jakarta: Raja Grafindo Persada, 2005.

[7] S. S. M. Sugeng, *Hukum Telematika Indonesia*. Jakarta: Kencana, 2020.

[8] Dr. Kasmir, *Bank dan lembaga keuangan lainnya*. Rajawali Pers, 2014.

[9] R. Usman, *Aspek-Aspek Hukum Perbankan Di Indonesia*. Jakarta: Gramedia Utama, 2001.

[10] M. P. Takasenseran, "'Perjanjian Antara Bank dan Nasabah Menurut Undang-Undang Nomor 10 Tahun 1998,'" *Lex Soc.*, vol. No. IV, no. No. 7.
[11] T. Widiyono, *Aspek Hukum Operasional Transaksi Produk Perbankan di Indonesia*. Bogor: Ghalia Indonesia, 2006.
[12] R. U. Djoni S Ghazali, *Hukum Perbankan*. Sinar Grafika, 2010.
[13] J. A. d. A. Safa'at, *Teori Hans Kelsen Tentang Hukum*. Jakarta: MKRI, 2006.
[14] M. Rani, "'Perlindungan Otoritas Jasa Keuangan Terhadap Kerahasiaan dan Keamanan Data Pribadi Nasabah Bank,'" *J. Selat*, vol. Vol. 2, no. No. 1, 2014.