






Legal Protection For Bank Customers In The Use Of E-Kyc In Opening New Accounts Online As A Form Of Digital Financial Innovation (Study At The Jakarta Head Office Of The State Savings Bank)

Jenrico Louis Hutabarat  
Universitas Sumatera Utara

Sunarmi 
Universitas Sumatera Utara

Detania Sukarja 
Universitas Sumatera Utara

Syarifah Lisa Andriati 
Universitas Sumatera Utara

 jenrico.hutabarat94@gmail.com

Abstract

This research examines the function of E-KYC in Indonesian banking, the responsibility of banks to protect customers' personal data, and the form of data protection at BTN Jakarta Head Office, using analytical descriptive normative legal methods with a statutory approach. POJK Number 23/POJK.01/2019 allows customer verification through electronic means to replace direct meetings, where E-KYC is implemented as Customer Due

Diligence which includes electronic identification, verification, and monitoring. The E-KYC organizing bank is required to meet the aspects of security, interconnectivity, system compatibility, technical support, and guarantee of service sustainability to be registered as a PSE, with sanctions from warnings to license revocation if negligent, as has been applied by BTN Mobile, which is registered as a domestic private PSE with international standard security technology to bridge the principle of knowing the customer and the right to privacy.

Keywords

E-KYC, BTN Mobile, Personal Data Protection.

Introduction

Banking institutions are one of the financial systems of a country. The important role of banks is seen as having strategic value as intermediaries for parties who have excess funds (surplus of funds) with parties who lack and need funds (lack of funds) thus banks will be engaged in credit activities and various services provided to serve financing needs and launch payment system mechanisms for all sectors of the economy.¹

Banks are financial institutions that are a place for individuals, private business entities, state-owned enterprises and also government institutions to save their funds through various service activities provided and serve the need for financing, launching a payment system for all sectors of the economy. Banks as a financial institution that collects funds from the public in the form of savings and deposits, and carries out its activities based on public trust, must truly maintain public trust.²

¹ Muhammad Djumhana, *Hukum Perbankan di Indonesia*, (Bandung: PT Citra Aditya Bakti, 2006), hlm. XV.

² Chairil Susanto, *Legal Opini*, Jurnal Ilmu Hukum, Vol.2 No.5, Tahun 2014, hlm 10.

Banks are not only tasked with collecting public funds in the form of deposits directly to channel them back to the community, but are obliged to maintain the confidentiality of their customers' data as consumers.³ Banking institutions are also an agent of trust from the public or customers given the existence of one of the principles of bank management, namely the principle of trust (fiduciary principle), so that banks in providing loans in the form of credit are always guided by the prudential banking principle.⁴

According to Hikmahanto Juwana, the banking industry has special characteristics that can be seen from two things, namely banking is one of the subsystems of the financial services industry, and banking is also an industry that relies heavily on public trust. One of the ways banks run their business is by collecting public funds as customers. So that banks are institutions that rely on public funds, and banks also have a burden on public trust in the way funds are managed so as not to cause losses to the community. As a result, banks must apply the prudential principle in managing their business. This prudential principle aims to maintain the trust of the depositing public and the creation of healthy banking.⁵

In relation to the application of the principle of prudential banking in regulating the traffic of banking activities, one of the efforts so that the principle can be applied is the application of the know your

³ Sentosa Sembiring, *Hukum Perbankan*. (Bandung: CV Mandar Maju, 2012), Hlm. 2.

⁴ Lukmanul Hakim, "Analisis Alternatif Penyelesaian Sengketa Antara Pihak Nasabah Dengan Industri Jasa Keuangan Pada Era Otoritas Jasa Keuangan", *Jurnal Keadilan Progresif*, Vol.6 No.2, Tahun 2015. Hlm. 162.

⁵ Devy Kusuma Wati, KYC Sebagai Peran Perbankan Dalam Pemberantasan TPPU, https://www.ppatk.go.id/siaran_pers/read/968/kyc-sebagai-peran-perbankan-dalam-pemberantasan-tppu.html, diakses tanggal 23 Mei 2023.

customer principle.⁶ The application of the Know You Customer (KYC) principle by banks can be seen in the creation of new accounts by customers, namely to determine the identity of customers, monitor customer transaction activities including reporting suspicious transactions or large transactions.⁷ KYC principles are realized through the implementation of customer acceptance policies, customer identification policies and procedures, monitoring of customer accounts and transactions, and risk management.⁸

Individuals have the right to determine whether or not to share or exchange their personal data. In addition, individuals also have the right to determine the conditions under which the transfer of personal data will take place. Furthermore, personal data protection also relates to the concept of the right to privacy. The right to privacy has evolved so that it can be used to formulate the right to protect personal data.⁹ In this case, Law Number 27 of 2022 concerning Personal Data Protection regulates that Personal Data Subjects are entitled to obtain information about the clarity of identity, the basis of legal interests, the purpose of requesting and using Personal Data and the accountability of the party requesting Personal Data.¹⁰ Adequate protection of Personal Data will be able to give the public confidence to provide Personal Data for the benefit of the greater community without being abused or violating their personal rights so that it will create a balance

⁶ *Ibid.*

⁷ Pasal 1 ayat 2 Peraturan Bank Indonesia nomor 3/10/PBI tahun 2001.

⁸ *Ibid.*, Pasal 2 ayat 2.

⁹ *Human Rights Committee General Comment No. 16 (1988) on the right to respect of privacy, family, home and correspondence, and protection of honour and reputation* (art. 17) seperti yang dikutip dalam Privacy International Report, 2013, hlm. 1-2.

¹⁰ Pasal 5 Undang-Undang Nomor 27 tahun 2022 tentang Perlindungan Data Pribadi.

between the rights of individuals and the community whose interests are represented by the state.¹¹

The utilization of information technology for the banking industry in the innovation of bank service products is also overshadowed by the potential risk of system failure and/or the risk of electronic crime (cybercrime) committed by irresponsible people. System failure can be caused by system malfunction (such as server down), and on a wider scale can be caused by natural disasters. Meanwhile, cybercrime that occurs in the banking industry in Indonesia tends to increase in Indonesia such as identity theft, carding, hacking, cracking, phishing, viruses, cybersquatting, ATM fraud, and others.¹²

In practice, consumers' personal information has been traded through agents without seeking prior permission from the information owner. A common case in Indonesia is the buying and selling of consumer data. Consumers whose data is successfully obtained become marketing targets for a company or individual product. Not a few internet users also offer account or follower buying and selling services. In fact, this practice opens up space for misuse of a person's data to commit crimes. Examples of data leaks that result in data misuse that have occurred in banking include the following:

1. On May 8, 2023, Bank Syariah Indonesia experienced a ransomware attack by the hacker group Lockbit 3.0. The perpetrators claimed to have stolen 1.5 terabytes of customer data, financial documents, legal documents, confidentiality

¹¹ Penjelasan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi.

¹² https://ditjenpp.kemenkumham.go.id/index.php?option=com_content&view=article&id=665:tanggung-jawab-penyelenggara-sistem-elektronik-perbankan-dalam-kegiatan-transaksi-elektronik-pasca-uu-no-11-tahun-2008&catid=107:hukum-teknologi-informasi&Itemid=187&lang=en , diakses pada tanggal 23 Mei 2023.

agreements, and passwords for internal access and company services.¹³

2. Data of two million BRI Life customers is suspected of being leaked and sold online. Information about the leak of BRI Life customer data was uploaded by a Twitter account on Tuesday, July 27, 2021. In the upload, it was written that the perpetrator threatened to sell sensitive data belonging to BRI Life. The hacker allegedly stole 250 gigabytes of the insurance company's customer data and sold it for US\$ 7,000 or IDR 101.5 million.¹⁴

Customer data leak incidents have the potential to cause the risk of loss of data subject reputation, loss of confidentiality and integrity of personal data, and potential financial loss. Banking data leaks cannot be separated from the level of security of the electronic system used. This means that Electronic System Organizers (in this case banks and third parties) have a crucial role in complying with the procedures for organizing electronic systems as stipulated in Government Regulation Number 71 of 2019 concerning the Implementation of Electronic Systems and Transactions. The hardware used by Electronic System Organizers must meet the following requirements:¹⁵

- a. Fulfilling the aspects of security, interconnectivity and compatibility with the system used;

¹³ Mediana, Kominfo Bersama BSSN Selidiki Insiden Kebocoran Data Pribadi BSI, <https://www.kompas.id/baca/ekonomi/2023/05/16/kominfo-akan-koordinasi-bssn-mendalami-insiden-kebocoran-data-pribadi-bsi>, diakses pada tanggal 23 Mei 2023.

¹⁴ Fransisca Christy Rosana, Kebocoran Data Nasabah BRI Life Bukti Lemahnya Proteksi dan Regulasi, <https://fokus.tempo.co/read/1488710/kebocoran-data-nasabah-bri-life-bukti-lemahnya-proteksi-dan-regulasi>, diakses pada tanggal 23 Mei 2023.

¹⁵ Pasal 7 ayat (1) Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik.

- b. Having technical support, maintenance and/or after-sales services from the seller or provider; and
- c. Having a guarantee of service continuity.

Fulfillment of these requirements must be done through certification or other similar evidence.¹⁶

Based on the background above, there are at least 3 (three) reasons why this research is important to be conducted: First, there is a conflict between the principle of knowing the customer and the right to privacy which should be bridged with personal data protection. Second, OJK Regulations have not accommodated regulations regarding Bank accountability in the event of a data leak. Third, the electronic system run by the Bank must have technical certification and there is no supervision in the context of overcoming data transaction leaks so that it can reduce efforts to protect customer data.

This study aims to discuss in depth the implementation of the principle of knowing your customer electronically at BTN Head Office Jakarta, which was chosen because it is the largest state-owned bank in the center of the Indonesian economy with high transaction complexity, with the formulation of the problem including: the function of E-KYC in organizing banking services in Indonesia, the legal responsibility of the Bank in protecting Customer Personal Data related to E-KYC practices, and the form of protection of Customer Personal Data implemented by BTN Head Office Jakarta in the implementation of E-KYC.

Method

¹⁶ Pasal 7 ayat (2) Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik.

The research method used is normative juridical, with a statute approach¹⁷ and case approach to study the use of e-KYC in opening new accounts online at BTN Head Office Jakarta. The research is descriptive in nature using secondary data as the main source, consisting of primary legal materials (legislation and interview results), secondary legal materials (books, research results, articles, journals), and tertiary legal materials (general dictionaries, legal dictionaries). Data collection techniques were carried out through literature studies and in-depth interviews with BTN Head Office Jakarta employees.¹⁸ Data analysis uses qualitative methods, by describing data in a quality manner in the form of regular, logical and systematic sentences to obtain conclusions that answer research problems.¹⁹

Result And Discussion

1. E-KYC as a Form of Implementation of the Principle of Prudence and Knowing the Customer in Bank Account Opening Services

Know Your Customer (KYC) in practice is implemented with the term Customer Due Diligence (CDD) which applies to every activity in the form of identification, verification and monitoring carried out by the Bank and ensures that the transaction is in accordance with the customer profile. The term CDD has the same meaning as KYC, namely understanding the character of the customer's transaction whether it is in accordance

¹⁷ Koto, I. (2024). The Potential Of Traditional Knowledge As An Improvement Of The Welfare Of Communal Communities. *DE LEGA LATA: Jurnal Ilmu Hukum*, 9(2), 162-169.

¹⁸ Fathin, F. J., & Koto, I. (2024). A Juridical Review of Transgender Heirs from the Perspective of Islamic Law and Civil Law. *JHR (Jurnal Hukum Replik)*, 12(2), 525-538.

¹⁹ Simatupang, R. S. A. (2024). Pelaksanaan Sistem Peradilan Pidana Anak Di Indonesia Perspektif Nilai Keadilan. *Jurnal Yuridis*, 11(1), 54-63.

with the profile or not, and if it is not in accordance, whether there is an element of suspicious transactions in the transaction.

Customer Due Diligence (CDD) is implemented in the form of a bank's obligation to identify potential customers to find out the potential customer's profile and verify the information and supporting documents of potential customers at the start of a business relationship.²⁰ Verification of the truth of the prospective customer's identity is carried out through a direct meeting (face to face) in order to ensure the truth of the prospective customer's identity.²¹ The verification process through direct meetings (face to face) can be replaced by verification through electronic means belonging to the bank or a third party that has received approval from the Financial Services Authority (OJK).²² Exceptions to verification through direct meetings are implemented with the following provisions:

- a. Verification is carried out through electronic processes and means owned by PJK and/or owned by prospective customers; and
- b. Verification must utilize population data that meets 2 (two) authentication factors.

Verification through electronic means is often referred to as Electronic-Know Your Customer (E-KYC).

Banks are required to identify and classify Prospective Customers or Customers into groups of individuals (natural persons), Corporations, and other legal arrangements.²³

²⁰ Pasal 17 ayat (1) POJK Nomor 23 /POJK.01/2019 tentang Perubahan Atas POJK Nomor 12/POJK.01/2017 tentang Penerapan Program Anti Pencucian Uang dan Pencegahan Pendanaan Terorisme di Sektor Jasa Keuangan.

²¹ Pasal 17 ayat (2) POJK Nomor 23 /POJK.01/2019 tentang Perubahan Atas POJK Nomor 12/POJK.01/2017 tentang Penerapan Program Anti Pencucian Uang dan Pencegahan Pendanaan Terorisme di Sektor Jasa Keuangan.

²² Pasal 17 ayat (3) dan (4) POJK Nomor 23 /POJK.01/2019 tentang Perubahan Atas POJK Nomor 12/POJK.01/2017 tentang Penerapan Program Anti Pencucian Uang dan Pencegahan Pendanaan Terorisme di Sektor Jasa Keuangan.

²³ Pasal 19 POJK Nomor 12/POJK.01/2017 tentang Penerapan Program Anti Pencucian Uang dan Pencegahan Pendanaan Terorisme di Sektor Jasa Keuangan.

Identification of Prospective Customers to find out the profile of Prospective Customers is done by requesting data and information which at least includes:²⁴

- a. For prospective customers who are individuals (natural persons):
 - 1) Identity containing:
 - a) full name including aliases (if any);
 - b) identity document number;
 - c) residential address according to identity document and other residential addresses (if any);
 - d) place and date of birth;
 - e) nationality;
 - f) occupation;
 - g) address and telephone number of workplace (if any);
 - h) gender; and
 - i) marital status;
 - 2) identity of the Beneficial Owner, if any;
 - 3) source of funds;
 - 4) average income per year; and
 - 5) the intent and purpose of the business relationship or transaction to be carried out by the Prospective Customer.

²⁴ Pasal 20 ayat (1) POJK Nomor 12/POJK.01/2017 tentang Penerapan Program Anti Pencucian Uang dan Pencegahan Pendanaan Terorisme di Sektor Jasa Keuangan.

For prospective customers who are natural persons, the above information must be supported by the prospective customer's identity documents and signature specimen.²⁵

b. for Prospective Corporate Customers:

- 1) name;
- 2) permit number from the authorized agency;
- 3) field of business or activity;
- 4) domicile address;
- 5) place and date of establishment;
- 6) form of legal entity or business entity;
- 7) identity of the Beneficial Owner if the Prospective Customer has a Beneficial Owner;
- 8) source of funds; and
- 9) intent and purpose of the business relationship or transaction to be carried out by the Prospective Customer.

For Prospective Corporate Customers in the form of companies classified as micro and small businesses plus:²⁶

- 1) signature specimen and power of attorney to the appointed party who has the authority to act for and on behalf of the company in conducting business relations with PJK;

²⁵ Pasal 21 POJK Nomor 12/POJK.01/2017 tentang Penerapan Program Anti Pencucian Uang dan Pencegahan Pendanaan Terorisme di Sektor Jasa Keuangan.

²⁶ Pasal 22 ayat (1) huruf a POJK Nomor 12/POJK.01/2017 tentang Penerapan Program Anti Pencucian Uang dan Pencegahan Pendanaan Terorisme di Sektor Jasa Keuangan.

- 2) NPWP card for Customers who are required to have NPWP in accordance with the provisions of laws and regulations; and
- 3) business permit or other documents required by the authorized agency.

For Prospective Corporate Customers in the form of companies that are not classified as micro and small businesses and for Prospective Customers other than Prospective Customers who are natural persons and Corporations in the form of companies, supplemented with the following supporting documents:²⁷

- 1) financial statements or descriptions of the company's business activities;
- 2) company management structure;
- 3) company ownership structure; and
- 4) identity documents of members of the Board of Directors or power of attorney of members of the Board of Directors who are authorized to represent the company to conduct business relations.

For Prospective Corporate Customers in the form of foundations, please provide the following supporting documents:²⁸

- 1) foundation activity permit;
- 2) description of foundation activities;

²⁷ Pasal 22 ayat (1) huruf b POJK Nomor 12/POJK.01/2017 tentang Penerapan Program Anti Pencucian Uang dan Pencegahan Pendanaan Terorisme di Sektor Jasa Keuangan.

²⁸ Pasal 22 ayat (3) huruf b POJK Nomor 12/POJK.01/2017 tentang Penerapan Program Anti Pencucian Uang dan Pencegahan Pendanaan Terorisme di Sektor Jasa Keuangan.

- 3) structure and name of foundation management; and
- 4) identity documents of management members or power of attorney from management members who are authorized to represent the foundation to conduct business relations with the Bank.

For Prospective Corporate Customers other than companies and foundations, whether they are legal entities or not, please provide the following supporting documents:²⁹

- 1) proof of permit from the authorized agency;
 - 2) name of the Corporation;
 - 3) deed of establishment and/or articles of association and bylaws (AD/ART); and
 - 4) identity document of the authorized party representing the Corporation in conducting business relations with the PJK.
- c. for prospective customers of other obligations (legal arrangements):
- 1) name;
 - 2) permit number from the authorized agency (if any);
 - 3) domicile address;
 - 4) form of agreement (legal arrangement);
 - 5) identity of the Beneficial Owner if the Prospective Customer has a Beneficial Owner;
 - 6) source of funds; and

²⁹ Pasal 23 ayat (2) huruf b POJK Nomor 12/POJK.01/2017 tentang Penerapan Program Anti Pencucian Uang dan Pencegahan Pendanaan Terorisme di Sektor Jasa Keuangan

- 7) intent and purpose of the business relationship or transaction to be carried out by the Prospective Customer.

For prospective customers in the form of other agreements (legal arrangements) plus the following supporting documents:³⁰

- 1) proof of registration with the authorized agency;
- 2) name of the agreement;
- 3) deed of establishment and/or articles of association and bylaws (AD/ART) (if any); and
- 4) identity document of the authorized party representing the other agreement (legal arrangement) in conducting business relations with the Bank.

- d. For prospective customers in the form of state institutions, government agencies, international institutions and foreign country representatives, PJK is required to request information regarding the name and address of the institution, agency or representative office.³¹ This information must be supported by documents including:³²

- 1) a letter of appointment for the authorized party representing the institution, agency or representative in conducting business relations; and

³⁰ Pasal 23 ayat (2) huruf c POJK Nomor 12/POJK.01/2017 tentang Penerapan Program Anti Pencucian Uang dan Pencegahan Pendanaan Terorisme di Sektor Jasa Keuangan.

³¹ Pasal 24 ayat (1) POJK Nomor 12/POJK.01/2017 tentang Penerapan Program Anti Pencucian Uang dan Pencegahan Pendanaan Terorisme di Sektor Jasa Keuangan.

³² Pasal 24 ayat (2) POJK Nomor 12/POJK.01/2017 tentang Penerapan Program Anti Pencucian Uang dan Pencegahan Pendanaan Terorisme di Sektor Jasa Keuangan.

- 2) specimen signature of the authorized party representing the institution, agency or representative in conducting business relations.

The Bank is required to verify the information and supporting documents of the Prospective Customer as referred to above, based on documents and/or other reliable and independent sources of information and ensure that the data is current.³³ Verification is carried out to ensure that the party acting for and on behalf of the Customer has obtained authorization from the Customer, and to identify and verify the identity of the party.³⁴ Mandatory verification is based on the risks of Money Laundering and/or Terrorism Financing that have been identified based on risk assessments conducted by the Bank.³⁵

The Bank may conduct interviews with Prospective Customers to examine and verify the validity and truth of documents, in the event of any doubt regarding the data, information and/or supporting documents received.³⁶ In case of doubt, the Bank is obliged to ask the Prospective Customer to provide more than one identity document issued by an authorized party to ensure the authenticity of the Prospective Customer's identity.³⁷ In the event that the Bank has implemented risk management procedures, the PJK may conduct business relations or transactions before the

³³ Pasal 25 ayat (1) POJK Nomor 12/POJK.01/2017 tentang Penerapan Program Anti Pencucian Uang dan Pencegahan Pendanaan Terorisme di Sektor Jasa Keuangan.

³⁴ Pasal 25 ayat (2) POJK Nomor 12/POJK.01/2017 tentang Penerapan Program Anti Pencucian Uang dan Pencegahan Pendanaan Terorisme di Sektor Jasa Keuangan.

³⁵ Pasal 25 ayat (3) POJK Nomor 12/POJK.01/2017 tentang Penerapan Program Anti Pencucian Uang dan Pencegahan Pendanaan Terorisme di Sektor Jasa Keuangan.

³⁶ Pasal 25 ayat (4) POJK Nomor 12/POJK.01/2017 tentang Penerapan Program Anti Pencucian Uang dan Pencegahan Pendanaan Terorisme di Sektor Jasa Keuangan.

³⁷ Pasal 25 ayat (5) POJK Nomor 12/POJK.01/2017 tentang Penerapan Program Anti Pencucian Uang dan Pencegahan Pendanaan Terorisme di Sektor Jasa Keuangan.

verification process is complete.³⁸ The verification process must be completed as soon as possible, after the customer's business relationship with the PJK occurs, taking into account that the risks of Money Laundering and Terrorism Financing can be managed effectively and that this direct meeting process does not disrupt normal business activities.³⁹

Banks are required to ensure that Prospective Customers, Customers, or WICs who open business relationships or conduct transactions act for themselves or for the benefit of the Beneficial Owner.⁴⁰ In the event that a Prospective Customer, Customer, or WIC acts in the interests of the Beneficial Owner, the Bank is required to carry out CDD towards the Beneficial Owner.⁴¹ In the case where the Beneficial Owner is classified as a Politically Exposed Person, the procedure applied is the EDD procedure.⁴² In the event that there is a difference in risk level between the Prospective Customer, Customer, or WIC and the Beneficial Owner, the implementation of CDD is carried out following the higher risk level.⁴³ The obligation to carry out CDD towards Beneficial Owners applies to prospective Customers, Customers or WICs who have a low risk level.⁴⁴

³⁸ Pasal 25 ayat (7) POJK Nomor 12/POJK.01/2017 tentang Penerapan Program Anti Pencucian Uang dan Pencegahan Pendanaan Terorisme di Sektor Jasa Keuangan.

³⁹ Pasal 25 ayat (5) POJK Nomor 12/POJK.01/2017 tentang Penerapan Program Anti Pencucian Uang dan Pencegahan Pendanaan Terorisme di Sektor Jasa Keuangan.

⁴⁰ Pasal 27 ayat (1) POJK Nomor 12/POJK.01/2017 tentang Penerapan Program Anti Pencucian Uang dan Pencegahan Pendanaan Terorisme di Sektor Jasa Keuangan.

⁴¹ Pasal 27 ayat (2) POJK Nomor 12/POJK.01/2017 tentang Penerapan Program Anti Pencucian Uang dan Pencegahan Pendanaan Terorisme di Sektor Jasa Keuangan.

⁴² Pasal 27 ayat (3) POJK Nomor 12/POJK.01/2017 tentang Penerapan Program Anti Pencucian Uang dan Pencegahan Pendanaan Terorisme di Sektor Jasa Keuangan.

⁴³ Pasal 27 ayat (4) POJK Nomor 12/POJK.01/2017 tentang Penerapan Program Anti Pencucian Uang dan Pencegahan Pendanaan Terorisme di Sektor Jasa Keuangan.

⁴⁴ Pasal 27 ayat (5) POJK Nomor 12/POJK.01/2017 tentang Penerapan Program Anti Pencucian Uang dan Pencegahan Pendanaan Terorisme di Sektor Jasa Keuangan.

2. Bank's Responsibility in Maintaining Customer's Personal Confidentiality in Relation to E-KYC Practices

The principle of confidentiality means that a customer's personal data must be kept confidential, especially in the era of digital banking. Based on Financial Services Authority Regulation Number 12/POJK.03/2018 concerning the Provision of Digital Banking Services by Commercial Banks, optimal utilization of information technology developments is a requirement to support innovation in banking services. Therefore, digital banking services are now increasingly used by banks. As a provider of digital banking services, of course, a bank must pay attention to the requirements as stipulated in Financial Services Authority Regulation Number 12/POJK.03/2021 concerning Commercial Banks, namely:

- a. have a business model with the use of innovative and safe technology in serving customer needs;
- b. have the ability to manage a prudent and sustainable digital banking business model;
- c. have adequate risk management;
- d. fulfill aspects of governance including the fulfillment of a Board of Directors who have competence in the field of information technology and other competencies in accordance with OJK provisions regarding the assessment of the ability and propriety of the main parties of financial services institutions;
- e. implement protection of customer data security; and
- f. provide efforts that contribute to the development of the digital financial ecosystem and/or financial inclusion.

Based on these requirements, it can be seen that customer data security is an important point in the implementation of digital banking services. The Banking Law as the basis for all banking services has also stipulated and provided legal protection for customer personal data, namely in Article 29 paragraph (4) of the Banking Law which states that for the benefit of customers, banks are required to provide information regarding the possibility of a risk of loss in connection with customer transactions carried out through the bank. Furthermore, provisions regarding bank confidentiality are also regulated in the provisions of Article 40 paragraph (1) of the Banking Law, namely that banks are required to keep confidential information regarding depositing customers and their deposits, except for tax purposes⁴⁵, accounts receivable settlement⁴⁶, judicial interests in criminal cases⁴⁷, exchange information between banks⁴⁸, and the party appointed by the customer or his heirs.⁴⁹

The provisions of bank secrecy in the Banking Law give rise to the logical consequence of criminal sanctions for those who violate it. The criminal sanctions for violations of bank secrecy are regulated in Articles 47 and 47 A of the Banking Law as follows:

Article 47 of the Banking Law reads:

⁴⁵ Lihat Pasal 41 UU Perbankan.

⁴⁶ Lihat Pasal 41 A UU Perbankan.

⁴⁷ Lihat Pasal 42 UU Perbankan.

⁴⁸ Lihat Pasal 44 UU Perbankan.

⁴⁹ Lihat Pasal 44 A UU Perbankan.

"(1) Anyone who, without a written order or permission from the Head of Bank Indonesia as referred to in Article 41, Article 41A and Article 42, intentionally forces a bank or Affiliated Party to provide information as referred to in Article 40, shall be subject to imprisonment for a minimum of 2 (two) years and a maximum of 4 (four) years and a fine of a minimum of IDR 10,000,000,000.00 (ten billion rupiah) and a maximum of IDR 200,000,000,000.00 (two hundred billion rupiah).

(2) Members of the Board of Commissioners, Directors, bank employees or other Affiliated Parties who intentionally provide information that must be kept confidential according to Article 40, shall be subject to imprisonment of at least 2 (two) years and a fine of at least IDR 4,000,000,000.00 (four billion rupiah) and a maximum of IDR 8,000,000,000.00 (eight billion rupiah)."

Article 47 A of the Banking Law reads:

"Members of the Board of Commissioners, Board of Directors, or bank employees who intentionally do not provide the information required as referred to in Article 42A and Article 44a, shall be subject to imprisonment for a minimum of 2 (two) years and a maximum of 7 (seven) years and a fine of a minimum of IDR 4,000,000,000.00 (four billion rupiah) and a maximum of IDR 15,000,000,000.00 (fifteen billion rupiah)."

In relation to the implementation of electronic systems and transactions, violations of the implementation of the principle of personal data protection may be subject to administrative sanctions.⁵⁰ The imposition of these sanctions is only aimed at parties who commit administrative violations, while violations of a moral or civil nature are not subject to administrative sanctions.⁵¹ The imposition of administrative sanctions can be in the form of:⁵²

- a. written warning;
- b. administrative fine;
- c. temporary suspension;
- d. termination of access; and/or
- e. removal from the list.

The provisions of sanctions stipulated by laws and regulations provide legal responsibility for banks to ensure that there are no leaks of bank secrets. Banks are therefore required to act in good faith in carrying out their business activities and to guarantee their business activities based on applicable banking standards.⁵³

The Financial Services Authority as a regulator, supervisor, examiner, and investigator in banking deposits can also help customers to obtain more certain legal protection. OJK's supervision of banking covers all aspects of a bank's operations, from institutional aspects, product and activity aspects, prudential aspects, to transparency aspects. This

⁵⁰ Pasal 100 ayat (1) Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik.

⁵¹ Penjelasan Pasal 100 ayat (1) Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik.

⁵² Pasal 100 ayat (2) Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik.

⁵³ Djumhana, *Hukum Perbankan di Indonesia*, (Bandung: Citra Aditya Bakti, 1996), hlm. 303-304.

supervision uses risk-based supervision strategies and methodologies to detect significant risks early and take appropriate and timely supervisory actions. The stages of supervision carried out by OJK include understanding the supervised bank, conducting bank risk assessments, preparing a supervision plan based on identified risks, conducting bank inspections, and monitoring bank conditions periodically. The legal protection provided by OJK to customers or consumers in banking is guided by Article 2 paragraph (1) of POJK Number 6/POJK.07/2022 concerning Consumer and Community Protection in the Financial Services Sector, namely by implementing the principles of: adequate education, openness and transparency of information, fair treatment and responsible business behavior, protection of assets, privacy and consumer data as well as effective and efficient handling of complaints and dispute resolution.

3. Protection of Personal Data of BTN Bank Customers, Central Branch, Jakarta in the Implementation of E-KYC

Personal Data of BTN Bank Customers obtained will be grouped into 4 categories, namely confidential personal data, restrictive personal data, general personal data and personal data for internal purposes, where each category is protected with a password to access it. Furthermore, the exchange or distribution of personal data is not permitted using social media by employees who are required to use Microsoft Things or via verified email for use by Bank Tabungan Negara. Each employee is also given a special user account to access the personal data, where the account password will be changed periodically.⁵⁴

Bank BTN through BTN Mobile ensures the security of its transactions and data storage by using three methods, namely

⁵⁴ Wawancara dengan Mohammad Anugrah Putra, Staf Compliance Management & Governance Division (CMGD) Bank BTN Cabang Pusat Jakarta, pada tanggal 8 Juni 2023.

first, BTN Mobile uses international standard security technology, namely by using the latest data security and encryption technology that meets international standards, namely the endpoint protection platform⁵⁵, Intrusion Detection System (IDS)⁵⁶, Security Incident and Event Management (SIEM)⁵⁷, Web Application Firewall (WAF)⁵⁸, and Privilege Access Management (PAM)⁵⁹. Second, BTN Mobile implements layered data isolation and protection by asking customers to enter PIN, password, CVV, and OTP (one time password) repeatedly on the application. Third, BTN Mobile has been supervised by Bank Indonesia (BI) and the Financial Services Authority (OJK). This supervision exists because BTN Mobile is a supporting application for banking services owned by Bank BTN. The purpose of this supervision is so that all financial services activities in the financial services sector are carried out regularly, fairly, transparently, and accountably, and are able to realize a

⁵⁵ *Endpoint protection platform* adalah solusi keamanan yang digunakan pada perangkat perusahaan untuk mencegah serangan dunia maya, mendeteksi aktivitas berbahaya, dan memberikan kemampuan remediasi instan.

⁵⁶ *Intrusion Detection System* atau IDS adalah sebuah sistem yang memonitor trafik jaringan untuk mendeteksi aktivitas-aktivitas mencurigakan. Jika aktivitas mencurigakan tersebut ditemukan, IDS akan melaporkannya dalam bentuk peringatan. Dengan kata lain, IDS bisa dibilang sebagai perangkat lunak pemindai sistem atau jaringan guna terhindar dari kegiatan yang melanggar kebijakan.

⁵⁷ *Security Incident and Event Management* (SIEM) merupakan sistem yang membantu anda untuk memonitor lalu lintas jaringan dan memberikan analisa secara real-time dari log yang dihasilkan oleh aplikasi ataupun perangkat keamanan.

⁵⁸ *Web Application Firewall* (WAF) merupakan aplikasi Firewall untuk aplikasi HTTP yang berfungsi untuk melindungi website secara spesifik dari ancaman serangan berbasis web dalam lapisan aplikasi.

⁵⁹ *Privileged access management* (PAM) adalah sistem keamanan identitas yang membantu melindungi organisasi dari ancaman cyber dengan memantau, mendeteksi, dan mencegah akses istimewa yang tidak sah ke sumber daya penting.

financial system that grows sustainably and stably, and is able to protect the interests of consumers and the community.⁶⁰

Customers can also contact the 24-hour Call Center to handle complaints from BTN customers who have implemented 3 Lines of Defense (LD) in cybersecurity governance such as IT Security (1.5 LD), IT Risk and IT Compliance (2 LD) and IT Audit (3 LD). Every e-Channel initiative and IT capability development, he said the company always carries out information security reviews and obtains approval from the Financial Services Authority (OJK) and the bank. In this case, Bank BTN has adopted the provisions of the OJK regulator POJK No.11/POJK.05/2022 concerning the Implementation of Information Technology by Commercial Banks.⁶¹

In relation to customer data protection, the BTN Mobile electronic system has been registered as a domestic private Electronic System Provider (PSE) by the Ministry of Communication and Information with PSE Registration Number: 001813.06/DJAI.PSE/12/2021 dated December 21, 2021.⁶² Regarding cyberspace security, Bank BTN collaborates with the National Cyber and Crypto Agency (BSSN) to cooperate in protecting information and electronic transactions based on the Memorandum of Understanding between PT. Bank Tabungan Negara (Persero), Tbk and the National Cyber and

⁶⁰ Wawancara dengan Mohammad Anugrah Putra, Staf Compliance Management & Governance Division (CMGD) Bank BTN Cabang Pusat Jakarta, pada tanggal 8 Juni 2023.

⁶¹ *Ibid.*

⁶² Direktorat Tata Kelola Aptika Kementerian Komunikasi dan Informatika, *Daftar PSE Domestik*, <https://psc.kominfo.go.id/tdpse-detail/2826> , diakses pada tanggal 11 Juni 2023, pukul 19.53 WIB.

Crypto Agency concerning the Protection of Information and Electronic Transactions Number 28/MOU/DIR/2022, Number PERJ.631/KABSSN/HK.07.01/09/2022 dated September 25, 2022.⁶³ The existence of registration as a domestic private Electronic System Provider (PSE) proves that the implementation of BTN Mobile has met the minimum requirements as stipulated in the provisions of Government Regulation Number 71 of 2019 concerning the Implementation of Electronic Systems and Transactions.

The supporting factors for the development of BTN Mobile are as follows:⁶⁴

- a. Information security is one of the pillars whose implementation and investment continues to be improved, including people, processes, and technology.
- b. Acceleration of the addition of payment and purchasing service features on all digital service channels by implementing efficient and effective partnership and application development processes.
- c. From the technology side, security uses the latest technology such as data at rest (encryption and data masking), data on transit (data security on the internet network or VPN) and data at use (anti-dumping technology or data lost prevention).

⁶³ Badan Siber dan Sandi Negara, *BSSN dan BTN Sepakati Kolaborasi untuk Tingkatkan Keamanan Transaksi Elektronik*, <https://bssn.go.id/bssn-dan-btn-sepakati-kolaborasi-untuk-tingkatkan-keamanan-transaksi-elektronik/>, diakses pada tanggal 11 Juni 2023, pukul 19.57 WIB.

⁶⁴ Wawancara dengan Mohammad Anugrah Putra, Staf Compliance Management & Governance Division (CMGD) Bank BTN Cabang Pusat Jakarta, pada tanggal 8 Juni 2023.

- d. From the process side, testing or drill test or pentest to assess whether security on the technology side is effective involving 3 tiers, namely IT, Risk and Compliance, and Audit.
- e. From the human resources aspect, BTN provides routine socialization to internal teams and also to customers to help protect data related to transactions such as account numbers, PINs, Passwords, and other personal data.

Meanwhile, the factors inhibiting the development of BTN Mobile are as follows:⁶⁵

- a. The use of gadgets is dominated by millennials born between 1990 and early 2000. There are still many older people who still choose conventional banking services because they do not know how to use gadgets, which has an impact on the use of electronic-based banking services.
- b. Public trust in the security system, especially regarding personal data information, is not evenly distributed across all levels of society, this is influenced by cases of account hacking or the spread of personal data information that is detrimental to customers;
- c. The market is limited only to internet users who are generally middle to upper class and educated; and
- d. The internet network is not evenly distributed throughout Indonesia.

⁶⁵ *Ibid.*

In order to anticipate the impact of acceptable risks, customers must also take part in maintaining the security of their personal data, namely by educating themselves about the importance of maintaining personal data information. This education can be obtained through the bank, such as staff, crew, sales, service points, and others. Currently, channels and campaigns that provide information about the misuse of personal data have also been widely carried out. So that customers can know how to protect their personal data, such as not sharing passwords, not sharing PINs, not sharing OTP codes, and not using passwords that are too easy such as birth dates.⁶⁶

The loss of customer funds or the spread of personal data in digital banking applications can be caused by various factors, both from errors on the part of the bank, the customer, or due to errors on the part of a third party. Of course, the losses experienced by the customer must be resolved in the form of accountability. The accountability given also varies according to the cause of the problem that occurs.

Bank BTN has established several complaint channels that can be accessed for customers to submit written or verbal complaints, namely the contact center 150286/1500286, website: www.btn.co.id, whatsapp +6287771500286, email: btncontactcenter@btn.co.id, and Bank BTN's official social media. Customers who submit complaints will be verified by Bank BTN and then the customer will receive a complaint number. Bank BTN will follow up and resolve the complaint and

⁶⁶ *Ibid.*

if the customer does not agree with the results of the settlement, they can continue the process at the Alternative Dispute Resolution Institution for the Financial Services System (LAPS SJK) or the judiciary. This is in accordance with the provisions of POJK Number 6/POJK.07/2022 concerning Consumer and Community Protection in the Financial Services Sector.

Bank BTN is obliged to be responsible for Consumer losses arising from errors, negligence, and/or actions that are contrary to the provisions of laws and regulations in the financial services sector, carried out by the Board of Directors, Board of Commissioners, Employees, and/or third parties who work for or represent the interests of Bank BTN. Bank BTN as an electronic system organizer is legally responsible for the implementation of the electronic system. The parties responsible for all legal consequences in the implementation of electronic transactions are:⁶⁷

- a. if done alone, all legal consequences in the implementation of Electronic Transactions are the responsibility of the parties to the transaction;
- b. if a power of attorney is given, all legal consequences in the implementation of Electronic Transactions are the responsibility of the grantor of the power of attorney; or
- c. if done through an Electronic Agent, all legal consequences in the implementation of Electronic

⁶⁷ Lihat Pasal 21 Undang-Undang Nomor 11 Tahun 2018 tentang Informasi dan Transaksi Elektronik sebagaimana diubah dengan Undang-Undang Nomor 19 Tahun 2016.

Transactions are the responsibility of the Electronic Agent organizer.

Bank BTN's responsibility for losses experienced by customers is to assist in the customer complaint process and conduct examinations/investigations in accordance with bank procedures and assist customers in finding solutions to losses experienced by customers such as making reports to the police for further handling. Bank BTN is also responsible for the maintenance of the BTN Mobile application to maintain the security and comfort of its customers in the future. Bank BTN will deactivate BTN Mobile access via the site to minimize the risk of social engineering attempts by cybercriminals. In addition, Bank BTN has also implemented a one-connected device policy to protect customers' BTN Mobile accounts. This is done so that BTN Mobile account owners can only access and transact using their accounts via one verified device.

Conclusion

E-KYC is implemented through Customer Due Diligence which includes identification, verification, and electronic monitoring to ensure that transactions match customer profiles, where banks must meet aspects of security, interconnectivity and compatibility, with BTN Mobile having been registered as a domestic private PSE number 001813.06/DJAI.PSE/12/2021 which implements international standard security technology, layered data protection, and supervision by BI and OJK. Meanwhile, there are still many customers who do not understand the importance of protecting personal data so that socialization is needed by the government and banks, which must implement clean and clear governance and always strive for the best

security system to mitigate risks and prevent misuse of customer data by irresponsible parties.

References

- Badan Siber dan Sandi Negara. "BSSN dan BTN Sepakati Kolaborasi untuk Tingkatkan Keamanan Transaksi Elektronik." <https://bssn.go.id/bssn-dan-btn-sepakati-kolaborasi-untuk-tingkatkan-keamanan-transaksi-elektronik/>. Diakses pada 11 Juni 2023.
- Bank Indonesia. (2001). *Peraturan Bank Indonesia nomor 3/10/PBI tahun 2001*.
- Bank Indonesia. (1999). *Undang-Undang Nomor 23 Tahun 1999 tentang Bank Indonesia* sebagaimana diubah dengan Undang-Undang Nomor 3 Tahun 2004 dan terakhir kali diubah dengan Undang-Undang Nomor 4 Tahun 2023 tentang Pengembangan dan Penguatan Sektor Keuangan.
- Direktorat Tata Kelola Aptika Kementerian Komunikasi dan Informatika. "Daftar PSE Domestik." <https://pse.kominfo.go.id/tdpse-detail/2826>. Diakses pada 11 Juni 2023.
- Djumhana, Muhammad. *Hukum Perbankan di Indonesia*. Bandung: Citra Aditya Bakti, 1996.
- Djumhana, Muhammad. *Hukum Perbankan di Indonesia*. Bandung: PT Citra Aditya Bakti, 2006.
- Fathin, F. J., & Koto, I. (2024). A Juridical Review of Transgender Heirs from the Perspective of Islamic Law and Civil Law. *JHR (Jurnal Hukum Replik)*, 12(2), 525-538.
- Hakim, Lukmanul. "Analisis Alternatif Penyelesaian Sengketa Antara Pihak Nasabah Dengan Industri Jasa Keuangan Pada Era Otoritas Jasa Keuangan." *Jurnal Keadilan Progresif*. Vol.6 No.2, 2015.
- Human Rights Committee General Comment No. 16 (1988) on the right to respect of privacy, family, home and correspondence, and protection of honour and reputation (art. 17). *Privacy International Report*, 2013.

- Kementerian Hukum dan HAM. "Tanggung Jawab Penyelenggara Sistem Elektronik Perbankan dalam Kegiatan Transaksi Elektronik Pasca UU No. 11 Tahun 2008." https://ditjenpp.kemenkumham.go.id/index.php?option=com_content&view=article&id=665:tanggung-jawab-penyelenggara-sistem-elektronik-perbankan-dalam-kegiatan-transaksi-elektronik-pasca-uu-no-11-tahun-2008&catid=107:hukum-teknologi-informasi&Itemid=187&lang=en. Diakses pada 23 Mei 2023.
- Kementerian Komunikasi dan Informatika. (2019). *Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik*.
- Koto, I. (2024). The Potential Of Traditional Knowledge As An Improvement Of The Welfare Of Communal Communities. *DE LEGA LATA: Jurnal Ilmu Hukum*, 9(2), 162-169.
- Kusuma Wati, Devy. "KYC Sebagai Peran Perbankan Dalam Pemberantasan TPPU." https://www.ppatk.go.id/siaran_pers/read/968/kyc-sebagai-peran-perbankan-dalam-pemberantasan-tppu.html. Diakses pada 23 Mei 2023.
- Mediana. "Kominfo Bersama BSSN Selidiki Insiden Kebocoran Data Pribadi BSI." <https://www.kompas.id/baca/ekonomi/2023/05/16/kominfo-akan-koordinasi-bssn-mendalami-insiden-kebocoran-data-pribadi-bsi>. Diakses pada 23 Mei 2023.
- Otoritas Jasa Keuangan. (2016). *Peraturan Otoritas Jasa Keuangan Nomor 55/POJK.03/2016 Tentang Penerapan Tata Kelola Bagi Bank Umum*.
- Otoritas Jasa Keuangan. (2017). *Peraturan Otoritas Jasa Keuangan Nomor 12/POJK.01/2017 tentang Penerapan Program Anti Pencucian Uang dan Pencegahan Pendanaan Terorisme di Sektor Jasa Keuangan*.
- Otoritas Jasa Keuangan. (2018). *Peraturan Otoritas Jasa Keuangan Nomor 12/POJK.03/2018 tentang Penyelenggaraan Layanan Perbankan Digital Oleh Bank Umum*.
- Otoritas Jasa Keuangan. (2019). *Peraturan Otoritas Jasa Keuangan Nomor 23/POJK.01/2019 tentang Perubahan Atas POJK Nomor*

12/POJK.01/2017 tentang Penerapan Program Anti Pencucian Uang dan Pencegahan Pendanaan Terorisme di Sektor Jasa Keuangan.

Otoritas Jasa Keuangan. (2022). *Peraturan Otoritas Jasa Keuangan Nomor 6/POJK.07/2022 Tentang Perlindungan Konsumen dan Masyarakat di Sektor Jasa Keuangan.*

Putra, Mohammad Anugrah. Wawancara dengan Staf Compliance Management & Governance Division (CMGD) Bank BTN Cabang Pusat Jakarta. 8 Juni 2023.

Republik Indonesia. (1945). *Undang-Undang Dasar Negara Republik Indonesia Tahun 1945.*

Republik Indonesia. (1992). *Undang-Undang Nomor 7 Tahun 1992 Tentang Perbankan* sebagaimana diubah dengan Undang-Undang Nomor 10 Tahun 1998 dan terakhir kali diubah dengan Undang-Undang Nomor 4 Tahun 2023 tentang Pengembangan dan Penguatan Sektor Keuangan.

Republik Indonesia. (1999). *Undang-Undang Nomor 39 tahun 1999 tentang Hak Asasi Manusia.*

Republik Indonesia. (2002). *Undang-Undang Nomor 15 Tahun 2002 tentang Tindak Pidana Pencucian Uang* sebagaimana diubah dengan Undang-Undang Nomor 25 Tahun 2003 dan terakhir kali dicabut dengan Undang-Undang Nomor 8 Tahun 2010 tentang Pencegahan dan Pemberantasan Tindak Pidana Pencucian Uang.

Republik Indonesia. (2006). *Undang-Undang Nomor 23 Tahun 2006 tentang Administrasi Kependudukan* sebagaimana diubah dengan Undang-Undang Nomor 24 Tahun 2013.

Republik Indonesia. (2008). *Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik* sebagaimana diubah dengan Undang-Undang Nomor 19 Tahun 2016.

Republik Indonesia. (2010). *Undang-Undang Nomor 8 Tahun 2010 tentang Pencegahan dan Pemberantasan Tindak Pidana Pencucian Uang.*

Republik Indonesia. (2011). *Undang-Undang Nomor 21 Tahun 2011 tentang Otoritas Jasa Keuangan.*

Republik Indonesia. (2022). *Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi.*

- Republik Indonesia. (2023). *Undang-Undang Nomor 4 Tahun 2023 tentang Pengembangan dan Penguatan Sektor Keuangan*.
- Rosana, Fransisca Christy. "Kebocoran Data Nasabah BRI Life Bukti Lemahnya Proteksi dan Regulasi." <https://fokus.tempo.co/read/1488710/kebocoran-data-nasabah-bri-life-bukti-lemahnya-proteksi-dan-regulasi>. Diakses pada 23 Mei 2023.
- Sembiring, Sentosa. *Hukum Perbankan*. Bandung: CV Mandar Maju, 2012.
- Simatupang, R. S. A. (2024). Pelaksanaan Sistem Peradilan Pidana Anak Di Indonesia Perspektif Nilai Keadilan. *Jurnal Yuridis*, 11(1), 54-63.
- Soekanto, Soerjono. *Pengantar Penelitian Hukum*. Jakarta: Universitas Indonesia Press, 2007.
- Susanto, Chairil. "Legal Opini." *Jurnal Ilmu Hukum*. Vol.2 No.5, 2014.