

PROTECTION OF CUSTOMER PERSONAL DATA OF BANK SYARIAH INDONESIA REVIEWED FROM POJK NUMBER 6/POJK.07/2022

Amandha Bayu Wiedyasari

University of Muhammadiyah Surakarta
Amandhabyw3030@gmail.com

Wardah Yuspin

University of Muhammadiyah Surakarta
wy204@ums.ac.id

ABSTRACT

This research aims to study and analyze the legal protection of Bank customer' data as arranged in POJK No. 6/POJK.07/2022 and analyze the case of leakage of customer personal data of Bank Syariah Indonesia based on POJK No. 6/POJK.07/2022. The method used is qualitative research with a normative legal approach. The results determine personal data consists of private information, which needs to be protected by banking institutions as institutions rely on public trust for their sustainability. Consumers and the Public have legal protection from the leakage of customer personal data, as outlined in OJK Regulation No. 06/POJK.07/2022 concerning Legal Protection in the Financial Services Sector. This regulation aimed to strengthen consumer protection aspects, including the protection of bank customers' data as financial service consumers. This regulation emphasizes the prohibition of providing consumers' data to third parties. This regulation includes rules on legal sanctions for parties that fail to comply with the provisions, such as provisions regarding the prohibition for financial service providers to misuse consumers' data or information. Sanctions imposed include administrative sanctions and nominal fines. Cases of leakage of customer data from Bank Syariah Indonesia can get legal sue due to the leakage of customer personal data in banking services against cyber crimes. PT. Bank Syariah Indonesia must compensate customers for damages caused by system malfunctions and unlawful acts. Bank Syariah Indonesia must be responsible for the leakage of customer data without the need for proof of fault.

Keywords: Consumer Protection, Customer Personal Data, Bank Syariah Indonesia.

INTRODUCTION

Banking activities are one of the institutions needed by society. Banking institutions become partners in fulfilling the needs of society, such as a place to store money, make investments, send large or small amounts of money, make payments, and so on. The majority of financial institutions, including banks, play a central role in the financial system. In addition to serving as fund collectors for the public, banking also reallocates funds back into loan products. In banking, individuals or legal entities that benefit from banking products and services are referred to as customers. This includes various activities such as purchases, utilization of

services, and leasing. Customers or consumers in banking need to obtain protection. From a legal perspective, consumer protection needs to be safeguarded as it is part of a right.¹

In POJK Number 6/POJK.07/2022, it is explained that there is a need to improve the implementation of consumer protection by financial services providers (FSPs) to realize consumer protection in the financial services sector. FSPs are financial institutions that carry out activities in fund disbursement, fund raising, and fund management in the financial services sector. Article 1 paragraph (4) of POJK explains that “consumer and public protection is an effort to provide knowledge and understanding of products and/or services of FSPs that will be used or utilized by consumers and/or the public, and efforts to provide legal certainty to protect consumers in fulfilling consumer rights and obligations in the financial services sector.”²

Due to the rapid development of technology and information, consumer protection has now become an integral part of society, especially in major cities such as Indonesia.³ The increasing number of information technology users makes people consider personal data protection important. The sophistication of current technology narrows privacy boundaries, making personal data easily spread. Therefore, personal data protection becomes something important to consider. Issues regarding personal data have led the government to issue new regulations, namely the Personal Data Protection Law, namely POJK Number 6/POJK.07/2022. The purpose of enacting this regulation is to prioritize the perspective of personal data protection for the development of new technologies, thus promoting ethical responsibility in respecting human rights, which is expected to become one of the reference bases for implementing consumer data protection laws.⁴

Personal data is defined as any data about an individual, whether identified and/or identifiable separately or in combination with other information, whether directly or indirectly through electronic and/or non-electronic systems.⁵ Misuse of personal data constitutes an act that meets criminal elements such as elements of theft and fraud, as well as other criminal acts from both objective and subjective perspectives. With the fulfillment of these elements, administrative sanctions, civil sanctions, and criminal sanctions are not sufficient to accommodate the misuse of personal data, which is actually a form of perfect crime.

Various forms of violations of personal data include theft, dissemination, and use of personal data not belonging to oneself, including falsification of personal data, copying data and information of customer ATM cards (skimming) where skimming perpetrators withdraw funds elsewhere. Personal data leaks are very difficult to avoid due to the rapid digitization. One online media source also reported the trading of personal data of customers.⁶ Traded personal data can have many benefits, such as providing insurance, credit cards, or unsecured loans. The exact number of leaked personal data in Indonesia cannot be determined. However, last year in 2023, there was a case of leakage of customer data from Bank Syariah Indonesia (BSI) reported by a mass media outlet.

Based on data obtained by researchers from CNN Indonesia on Saturday, May 13, 2023, at 10:35 AM WIB, it was found that the case of leakage of customer data from Bank Syariah Indonesia (BSI) was suspected to involve 15 million customers. The leakage of customer data

¹Putri Annisya Chaerani. (2023). *Perlindungan Hukum Konsumen Atas Penyalahgunaan Data Pribadi Oleh Perusahaan Fintech Dalam Transaksi Peer To Peer Lending*. Jurnal Ilmiah.

²Amatul Najla. (2023). *Perlindungan Hukum Terhadap Konsumen Pinjaman Berbasis Online Oleh Otoritas Jasa Keuangan (Ojk) Berdasarkan Pojk Nomor 6/Pojk.07/2022*. Madani : Jurnal Ilmiah Multidisiplin, 1(8).

³Putri Annisya Chaerani. (2023). *Op.Cit.*

⁴Fadlia, D. H., & . Y. (2015). *Peran Otoritas Jasa Keuangan (Ojk) Dalam Perlindungan Hukum Bagi Investor Atas Dugaan Investasi Fiktif*. Law Reform, 11(2), 207. <https://doi.org/10.14710/Lr.V11i2.15768>

⁵Sahat Maruli Tua Situmeang, (2021), *Penyalahgunaan Data Pribadi Sebagai Bentuk Kejahatan Sempurna Dalam Perspektif Hukum Siber*. SASI, 1) 14).

⁶Nursantih, N., & Ratnawati, E. (2023). *Pengawasan Ojk Atas Data Pribadi Konsumen Pada Perusahaan Peer To Peer Lending*. 5(4). <https://doi.org/10.31933/Unesrev.V5i4>

from Bank Syariah Indonesia includes names, mobile phone numbers, addresses, account balances, account numbers, transaction histories, account opening dates, and job information. The data of Bank Syariah Indonesia customers was stolen by ransomware in the form of financial documents, legal documents, and passwords. This resulted in customers being unable to access BSI's mobile banking service and errors during cyber attacks. Additionally, based on information from *liputan6.com* on May 11, 2023, at 3:40 PM, it was found that there were illegal transactions in BSI's mobile banking that were not carried out by customers, and customer funds could take a considerable amount of time to be returned, but the security of their personal data was doubted after this incident. In this case, many consumers do not fully understand the latest legal regulations and do not bring this case to the appropriate legal authorities.⁷

Many people do not understand that Regulation No. 6/POJK.07/2022 regarding Consumer and Public Protection in the Financial Services Sector provides legal certainty to the public as consumers to protect all their personal data. With cases of misuse of personal data, it can be concluded that there are weaknesses in the system and a lack of supervision, resulting in losses for the owners of personal data. Misuse of all forms of personal data constitutes a violation of the law in the field of information technology and can also be categorized as a violation of human rights, as personal data is part of human rights that must be protected.⁸ FSPs are prohibited from providing personal data and/or information about Consumers to third parties, and FSPs are prohibited from offering products and/or services that harm or potentially harm prospective Consumers by abusing the situation or conditions of prospective Consumers and/or the public who have no other choice in making decisions. Legal protection related to personal data has essentially been established and enacted, but overall, enforcement is not yet maximal, so the personal data protection law is still general and subject to multiple interpretations.⁹

Research conducted by Guna Gerhat analyzing the role of the Financial Services Authority in banking as an effort to protect customers' personal data revealed that it is OJK's obligation to ensure customer protection and effective overall financial sector regulation to foster the economy in Indonesia. This aspect includes protection of customer's personal data, which must be kept confidential to maintain public trust in financial institutions.¹⁰ Research results from Pamela Herfesia Safsafubun on consumer protection analysis of their personal data in banking institutions explained that there are consumer data protection regulations used to fight personal data theft so that personal ownership rights can be protected.¹¹ Research results from Alga Soraja on legal protection of privacy and personal data rights from the perspective of human rights revealed that data is "the right to be alone" as a basic action or thought of privacy. Because protection of personal data is a constitutional right of all citizens, oversight is the respect and protection of this right. In Indonesia, it is necessary to protect personal data in accordance with laws and regulations. Oversight of personal data in Indonesia is usually regulated by a number of laws designed to protect personal data privacy. These laws and

⁷<https://www.liputan6.com/teknoread/5279997/ini-penyebab-aplikasi-bsi-error-nasabah-keluhkan-tak-bisa-akses-bsi-mobile>

⁸Fadlia, D. H., & . Y. (2015). Peran Otoritas Jasa Keuangan (Ojk) Dalam Perlindungan Hukum Bagi Investor Atas Dugaan Investasi Fiktif. *Law Reform*, 11(2), 207. <https://doi.org/10.14710/Lr.V11i2.15768>

⁹Saleh, Hm., Febryan Fitrahady, K., Zuhairi, A., Sutrisno, B., & Annisya Chaerani, P. (2023). Penyuluhan Tentang Penanganan Penyalahgunaan Data Pribadi Terhadap Nasabah Peer To Peer Lending Berdasarkan Hukum Positif Di Kecamatan Gunung Sari (Vol. 5).

¹⁰Gerhat Sinaga, G., Sulistiyanto Jusuf, A., Kornelius, Y., Desi, D., Tarina, Y., Hukum, F., Veteran, U. ., & Jakarta, . (2023). Analisis Peran Otoritas Jasa Keuangan Terhadap Perbankan Sebagai Upaya Perlindungan Data Pribadi Nasabah Bank (Studi Kasus Kebocoran Data Nasabah Bank Syariah Indonesia).

¹¹Pamelia Herfesia Safsafubun. (2023). Analisis Perlindungan Konsumen Terhadap Transaksi Elektronik Pada Lembaga Perbankan Berdasarkan Peraturan No. 6/Pojk.07/2022. *Jimps: Jurnal Ilmiah Mahasiswa Pendidikan Sejarah*, 4(1).

regulations can have positive impacts, such as economic value, increasing order and morality in society, and the state.¹²

From these various researches, there has not been any discussion regarding the protection of personal data of Bank Syariah Indonesia customers reviewed from POJK Number 6/POJK.07/2022. Previous research only examined the role of financial services authorities in banking as an effort to protect personal data and the importance of legal protection of customers' privacy and personal data but did not emphasize the legal regulations that deal with the protection of customers' personal data in accordance with POJK Number 6/POJK.07/2022. This is viewed from Bank Syariah Indonesia, which violated principles of data security, data privacy, and ethics. With the motif of data theft causing loss of confidentiality, privacy, availability, and integrity to PT. Bank Syariah Indonesia and resulting in losses both material and non-material, Therefore, based on the above problems, this research will discuss how the protection of customers's personal data in Indonesian Sharia banking institutions should be based on Regulation No. 6/POJK.07/2022. This is also one of the government's concrete actions in providing protection for consumers in Indonesia. Therefore, based on a brief presentation of consumer legal protection issues, this research aims to analyze the legal protection of customers's personal data from banks reviewed in POJK No. 6/POJK.07/2022 and cases of leakage of personal data from Bank Syariah Indonesia customers seen in POJK No. 6/POJK.07/2022.

METHOD

This research uses a qualitative research methodology. Qualitative research is a research procedure that generates descriptive data in the form of written or spoken words from individuals and observed behaviors. The qualitative research method has a detailed and flexible design, with the actual design being determined after the research is conducted. The nature of this research is normative legal research. The problem-solving approach used in this research is the statutory approach, by examining Regulation No. 6/POJK.07/2022, and the conceptual approach regarding consumer personal data protection in the financial services sector to address the role of financial services authorities in protecting consumers and society.

ANALYSIS AND DISCUSSION

Legal Protection of Customer Personal Data in Banks Reviewed from POJK No. 6/POJK.07/2022

Consumers are individuals who deposit their funds or utilize services in financial service institutions, such as bank customers, participants in pension funds, and investors in the capital market, based on regulations in the financial services sector. Consumer and societal protection is an effort involving understanding financial service products or services utilized by consumers or society as well as providing legal assurance to protect consumers in fulfilling their rights and obligations in the financial services sector.¹³

One of the bank's obligations is to ensure the confidentiality of customer personal data. Personal data is defined as any information related to identifying or potentially identifying an individual. Personal data is true and real information inherent to a person, enabling their identification. It encompasses various forms of information, whether directly or indirectly identifiable, such as citizenship numbers on ID cards, the names of biological parents, significant life events, etc.

In the *Kamus Besar Bahasa Indonesia* (Indonesian Dictionary), the definition of “data” is accurate and real information that can be used as a basis for study. Meanwhile, “pribadi” (personal) refers to humans as individuals (self or oneself). Therefore, it can be concluded that “data pribadi” (personal data) is accurate and real information owned by humans as individuals. According to John Locke’s theory, personal data is an inherent right bestowed upon all individuals by nature, encompassing the right to life, liberty, and property, which are their own and cannot be revoked or abridged by the state.¹⁴ With existing regulations serving as the basis for personal data protection, individual freedoms and confidentiality are human rights, whether concerning personal data or personal matters.¹⁵

Actually, personal data consists of all individual-related information and tends to be subjective. Protection of personal data falls within the realm of criminal law concerning the misuse of personal data, which can cause harm to individual victims. Whereas individuals are social units with undeniable rights and directed towards personal interest fulfillment, In cultural relativism models, a community is a social unit where concepts like individualism, freedom of choice, and equality are unknown.¹⁶ Hence, both society, communities, and governments need to understand the importance of awareness in safeguarding or protecting data and personal data to prevent easy exploitation by the public, as both data and personal data are part of privacy. Therefore, there needs to be strong legal enforcement in personal data protection.

Satjipto Rahardjo explains that legal protection of personal data is an effort to safeguard the human rights of those affected and is given to society to enjoy all rights granted by law. In line with Satjipto’s opinion, C.S.T. Kansil suggests that legal protection entails various legal efforts by law enforcement agencies to provide mental and physical security from disturbances and threats from any party. Furthermore, Moch. Isnaeni discusses the theory of legal protection, stating that the law seeks to create protective shields from potential damages that can strike at any moment.¹⁷

Law No. 27 of 2022 concerning Personal Data Protection, Article 1 Number 1, defines personal data as data about an individual that is identified or can be identified separately or in combination with other information, whether directly or indirectly, through electronic or non-electronic systems. And according to Law No. 23 of 2006 concerning Population Administration (“Population Administration Law”) as amended by Law No. 24 of 2013 concerning Amendments to Law No. 23 of 2006 concerning Population Administration (“Law 24/2013”). Article 1 number 22 of Law 24/2013 states: Personal data is specific individual data that is stored, maintained, and guarded for its accuracy and confidentiality. There is no clear legal definition of personal data in the ITE Law. However, from the official interpretation perspective of personal rights in Article 26 Paragraph (1), personal data includes personal life matters, including the communication history of an individual and data about an individual.¹⁸ And in Government Regulation No. 82 of 2012 concerning Electronic System and Transaction Providers, personal data is “specific individual data that is stored, maintained, kept accurate, and kept confidential” (Article 1 Paragraph 27).

Personal data is closely related to personal information, where personal data can reveal personal information about an individual. Personal information is defined as information that

¹⁴John Locke. (1964). *The Second Treatise of Civil Government and a Letter Concerning Toleration*, disunting oleh J.W. Gough, Blackwell, Oxford.

¹⁵Raymond Wacks, *Personal Information, Privacy and the Law*, Oxford: Clarendon Press, 1989, p.1-5.

¹⁶Philip Alston, (2008) *Hukum hak asasi manusia*, PUSHAM UII: Yogyakarta.

¹⁷Mirza Alvina Maharani (2022), *Perlindungan Nasabah Bank Syariah BUMN Pasca Merger Ditinjau Berdasarkan Hukum Perseroan Terbatas dan Hukum Perbankan*, *International Journal Of Sociology, Policy And Law (IJOSPL)* Vol. 3 No. 2

¹⁸Daniar Supriyadi. (2017) “Data Pribadi dan Dua Dasar Legalitas Pemanfaatannya”. <https://www.hukumonline.com/berita/baca/lt59cb4b3feba88/data-pribadi-dan-dua-dasar-legalitaspemanfaatannya-oleh--daniar-supriyadi/>. Diakses pada 16 Maret 2020. Pukul 18.04 WIB

identifies an individual, illustrating the connection between information and personal identity, whether sensitive or considered ordinary, which can identify a person. Personal information that can describe a person includes population data, bank account details, height, blood type, and fingerprints, which are inherent to an individual. And if that information is not tied to the individual who possesses it, then that information is not personal information.

In Law No. 27 of 2022 concerning Personal Data Protection, it is mentioned that personal data controllers and personal data processors include any person, any public entity, and international organizations. Banking institutions are obliged to protect all the personal data of their customers. According to Article 1 Number 1 of Law No. 10 of 1998 as amended by Law No. 7 of 1992 concerning Banking, banking is everything related to banks, including institutions, business activities, and methods and processes in conducting their business. Banking institutions rely on public trust for their business continuity. Thus, to maintain public trust in banks, the government must strive to protect the public as bank customers. If there is a decline in public trust in banking institutions, it would be a disaster for the country's economy as a whole, and such a situation would be difficult to recover from. Banking institutions are data controllers of customer personal data. Therefore, banks are responsible for all the personal data of their customers.

Article 20 states that personal data controllers must have a legal basis for processing personal data. And the legal basis for processing personal data as referred to in paragraph (1) includes: valid explicit consent from the personal data subject for one (one) or several specific purposes conveyed by the personal data controller to the personal data subject; fulfillment of contract obligations in the event the personal data subject is one party; or meeting the personal data subject's request when making a contract; and fulfillment of legal obligations of the personal data controller in accordance with the provisions of the laws and regulations. Therefore, personal data controllers need to truly safeguard customer personal data. And there needs to be strong legal enforcement in the event of personal data leaks.

Legal protection is an effort to protect the rights of legal subjects. Therefore, the emergence of POJK No. 6/POJK.07/2022 explains the need for improving the implementation of consumer protection by financial services providers to realize consumer and societal protection in the financial services sector. Banking service users, in particular, are entitled to legal protection concerning various consumer personal data. Therefore, the government must create regulations to ensure legal certainty for consumers and prevent any party from being harmed.

The basic principle in consumer protection is that service providers are required to adhere to fundamental principles such as transparency, fair treatment, reliability, confidentiality, data security, and swift, simple, and affordable consumer dispute resolution. The Financial Services Authority (OJK), within its authority, has enacted the Regulation of the Financial Services Authority of the Republic of Indonesia Number 6/POJK.07/2022 concerning Consumer and Community Protection in the Financial Services Sector on April 18, 2022, replacing the Regulation of the Financial Services Authority Number 1/POJK.07/2013 concerning Consumer Protection in the Financial Services Sector enacted on August 6, 2013.

OJK, in this regard, oversees financial services activities across various sectors such as banking, pension funds, insurance services, and other financial service institutions.¹⁹ However, overall, for all financial service sectors, including capital markets, insurance, pension funds, financing institutions, and other financial service institutions, including banking, to carry out its regulatory tasks, OJK is authorized to: establish legislation in the financial services sector;

¹⁹Otoritas Jasa Keuangan. (2015). Otoritas Jasa Keuangan, Workshop Perlindungan Konsumen Di Sektor Jasa Keuangan, Bidang Edukasi Perlindungan: Jakarta..

establish OJK regulations and decisions; establish regulations regarding supervision in the financial services sector; and establish various matters in the financial services sector.²⁰

The protection of consumer data privacy in bank customers reviewed in POJK No. 6/POJK.07/2022 is stated in Article 1 paragraph (4), which explains that “consumer and community protection is an effort to provide knowledge and understanding of financial services products and services to be used or utilized by consumers and/or the community, and efforts to provide legal certainty to protect consumers in fulfilling consumer rights and obligations in the financial services sector.”

This is because cases of misuse of personal data harm many consumers, proving the need for legal protection of consumer personal data. Allan Westin defines privacy as the right of individuals, groups, or institutions to determine whether information about them will be disclosed to others. Westin’s definition of privacy is called information privacy because it concerns personal information. Then one of the privacy concepts expressed by Thomas J. Imedinghaff is the privacy of data about a person, meaning that privacy rights can be attached to information about someone collected and used by others. This concept proves that data security is the embodiment of an individual’s privacy that must be protected.²¹

The determination of the latest OJK Regulation on Consumer and Society Protection in the Financial Services Sector aims to strengthen consumer protection aspects, including banking usage for various transactions in the community’s life as financial service consumers. The consumer protection principles established in the OJK Regulation include:

1. Adequate Education
2. Transparency and information disclosure
3. Fair treatment and responsible business behavior
4. Protection of Assets, Privacy, and Consumer Data
5. Effective and Efficient Complaint Handling and Dispute Resolution

According to these principles, the purpose of Regulation No. 6/POJK.07/2022 is to protect consumers and society in the financial services sector. These principles can be found in Article 2 as follows:

1. Accurate instructional data.
2. Clarity and Explanation of Data.
3. Fair and Considerate Treatment in Activities.
4. Security of Resources, Protection, and Buyer Data.
5. Serious and professional handling of complaints and inquiry purposes

In Article 4 of the OJK Regulation, it is stated that:

1. Financial service providers are required to act in good faith in carrying out their business activities.
2. Financial service providers are prohibited from giving discriminatory treatment to consumers.

Article 6 of the OJK Regulation also states:

- a. Financial service providers are expected to have and implement structured approaches and systems to follow and ensure buyer insurance.

²⁰Syukron. (2019). Pengantar Sistem Hukum Asuransi Syariah Dan Kepailitan Di Indonesia. Indramayu:Adab, 3(2).

²¹Benuf, (2019). Otoritas Jasa Keuangan Republik Indonesia. Refleksi Hukum Jurnal Ilmu Hukum, 3(2).

- b. Structured approaches and techniques related to customer security,
- c. as referred to in subsection (1), incorporating the following activities: a. product or service development. b. delivery of information related to products or services. c. communication of information about products and services. d. promotion activities for products and services. e. Arrangements related to goods or administration regulations. f. administration arrangements related to the use and benefit of goods or administration. g. handling complaints and resolution of inquiries related to goods or administration.
- d. Within the framework of the policies and written procedures mentioned in subsection (2), the following aspects are included: a. ensuring open access for all consumers. b. providing special services for consumers with special needs and the elderly. c. maintaining the security and protection of assets owned by consumers. d. protecting the confidentiality and privacy of consumer data and information. e. providing information about the handling and resolution of complaints filed by consumers. f. regulating mechanisms for the use of consumer data and personal information.²²

Article 8 covers the following:

1. Financial service providers (PUJK) have an obligation to be responsible for the losses experienced by consumers, caused by errors, negligence, and/or actions contrary to the provisions contained in the regulations in the financial services sector, which are carried out by the directors, board of commissioners, employees, and/or third parties who, in their implementation, represent the interests of the financial service provider.
2. To prove that there is involvement, error, negligence, and/or actions contrary to the regulations in the financial services sector carried out by the consumer, PUJK is not responsible for the losses experienced by the consumer.
3. The form of responsibility for the losses referred to in paragraph (1) has been agreed upon by both parties, namely the consumer and PUJK.
4. Follow-up by the Financial Services Authority in the process of proving, as referred to in paragraph (2), is carried out in accordance with the financial services authority regulations regarding the conduct of consumer service providers.

Articles 41 and 42 regulate the handling and resolution of disputes related to products and services provided by the OJK to consumers:

Article 41:

1. PUJK is not allowed to charge consumers for implementing service complaint policies and procedures.
2. OJK regulations govern the implementation of complaint services in accordance with the provisions regarding consumer complaints in the financial services sector.

Article 42:

²²Otoritas Jasa Keuangan Republik Indonesia. (2022). Otoritas Jasa Keuangan Republik Indonesia Nomor 6/Pojk.07/2022.

1. If consumers do not reach an agreement in filing a complaint with PUJK, they have the option to resolve the dispute alternatively or through litigation processes in the judicial institution.
2. Dispute resolution in the financial services sector outside the courts, as mentioned in paragraph (1), is carried out through LAPS (Financial Services Sector-Specific Alternative Dispute Resolution Institutions).

Consumer protection in the event of personal data leaks certainly involves legal aspects for people. This law is divided into two, namely:

1. Preventive legal protection Preventive legal protection is a form of legal protection where society is given the opportunity to raise objections or opinions before a government decision takes definitive shape and aims to prevent disputes. Preventive efforts are made by OJK to prevent violations that occur in the implementation of personal data breach systems.²³
2. Repressive Legal Protection Repressive legal protection is a form of legal protection more focused on dispute resolution. When consumers experience personal data breaches, OJK will provide legal protection. The substance of improvements to strengthen consumer and society protection included in Regulation No. 6/POJK.07/2022 includes:
 - a. Regulatory approaches to the product and/or service life cycle that increasingly optimize efforts to protect consumers and society from product and/or service design to dispute handling and resolution;
 - b. Strengthening the principle of consumer and society protection, including requiring PUJK to carry out “adequate education” to enhance consumers and society’s ability to choose financial service sector products and services;
 - c. Strengthening the implementation of the principle of transparency and information disclosure through regulations on forms, procedures, and exceptions for delivering summaries of product and service information.
 - d. Strengthening support for consumers and/or disabled and elderly society, as well as increasing consumer data and information protection;
 - e. Obligation to provide sufficient time for consumers to understand agreements before signing or a cooling-off period after signing agreements for products and services with long-term and/or complex terms;
 - f. Obligation to record if product and/or service offers are made through personal voice and/or video communication;
 - g. Affirmation of OJK’s authority in consumer protection, including market conduct supervision as the implementation of articles 28 to 30 of the OJK Law;
 - h. Obligation to establish a consumer and society protection unit or function;
 - i. Obligation to submit self-assessment reports by PUJK to OJK regarding compliance with consumer protection provisions²⁴

The latest OJK regulation also focuses on financial service providers who have financial products and/or services directly related to consumers. This OJK regulation also accommodates other financial service institutions that have been declared supervised by OJK based on relevant regulations (Financial Services Authority, 2022). This includes banking service

²³Abdurrazaq Triansyah, P. N. S. J. N. F. A. M. A. (2022). Peran Otoritas Jasa Keuangan Dalam Perlindungan Hukum Bagi Pengguna Pinjaman Online Ilegal (Studi Kasus Pinjol Ilegal Di Yogyakarta), 5(2).

²⁴Sekretariat Kabinet Republik Indonesia. (2023). Ojk Terbitkan Aturan Baru Perlindungan Konsumen. <https://Setkab.Go.Id/Ojk-Terbitkan-Aturan-Baru-Perlindungan-Konsumen>.

providers that have been licensed by OJK. The OJK regulation prohibits all financial service providers from providing consumer personal data to third parties. Consent must be obtained from the consumer if the financial service provider intends to share consumer personal data or information as a condition for the use of financial products or services. If a consumer terminates a financial product or service agreement, the financial service provider is not allowed to use the consumer's personal data or information. Personal data and information that must be protected under this OJK regulation include individual and corporate personal data and information. Individual personal data includes: name, National Identity Number (NIK), address, date of birth and/or age, telephone number, mother's name, and other data provided by the consumer to the financial service provider. Additionally, corporate personal data and information include: name, address, telephone number, composition of directors and board of commissioners, including identification cards, and other data provided to the financial service provider. This OJK regulation also stipulates the obligation of a financial service provider to provide written or oral explanations regarding the purpose and consequences of the consumer's agreement to provide access to their personal data and information. In managing consumer personal data and information, financial service providers must use reliable information technology to ensure the security of consumer personal data and information. If financial service providers obtain consumer personal data and information from other parties, they must have written statements that the concerned party has obtained consent from the consumer, and the financial service provider must also inform the consumer about the source of the personal data and information obtained by the financial service provider.

Compared with previous OJK regulations, this regulation has differences. The substance of personal data and information protection regulations in this latest OJK regulation is mentioned in detail and clearly. In addition to still including the protection of personal assets, privacy, and consumer data as one of the principles of consumer protection, the substance of personal data and information protection regulations is strengthened as part of the basic conduct rules for financial service providers. In addition to this OJK Regulation No. 06/POJK.07/2022, derivative regulations regarding the protection of customer personal data by OJK can also be found in Circular Letter of the Financial Services Authority No. 14/SEOJK.07/2014 Regarding the Confidentiality and Security of Customer Personal Data and/or Information.²⁵

The latest OJK regulation stipulates legal sanctions aimed at parties who do not comply with the provisions, one of which is the provision regarding the prohibition of financial service providers abusing consumer data and information. These sanctions take the form of administrative sanctions, namely written warnings, fines of a certain amount, revocation of business permits, revocation of product and service permits, prohibition as a principal party according to OJK regulations on reassessment for principal parties of financial services institutions, and restrictions or freezing of all forms of products, services, or business activities.

Administrative sanctions can be imposed with or without the prior imposition of written warnings. The imposition of sanctions in OJK Regulation No. 06/POJK.07/2022 includes repressive protective measures. Legal protection is protection in the form of sanctions imposed after a problem arises, such as fines, imprisonment, and other sanctions aimed at resolving the issue. Compared to previous OJK regulations, the regulation of sanctions does not cover sanctions directed at financial service providers who have misused consumer personal data. In those regulations, sanctions were only directed at violators who caused financial losses to their consumers, whether in banking, capital markets, pension funds, life insurance, financing, pawnshops, guarantees, or general insurance. Therefore, the sanctions listed in the previous

²⁵Ni Made Intan Pranita Dewanthara, M. G. S. K. R. (2020). Perlindungan Hukum Terhadap Pihak Pemberi Pinjaman Aki-
bat Terjadinya Gagal Bayar Peer To Peer Lending. *Jurnal Hukum Kenotariatan Fakultas Hukum Universitas Udayana*, 5(3).

OJK Regulation cannot be applied to personal data violators. Furthermore, in OJK Regulation No. 06/POJK.07/2022, the regulation also specifies the amount of fines imposed on violators, with a maximum of Rp. 15,000,000,000.00 (fifteen billion Indonesian Rupiah).

Case of Personal Data Leak of Customers of Bank Syariah Indonesia as Seen from POJK No. 6/POJK.07/2022

In the rapidly advancing era of digitalization, data leaks have become a serious issue across various sectors, particularly in the banking sector. Data breaches are not isolated incidents but rather serious and alarming problems. The dissemination of personal information about customers, such as account numbers, credit card information, identity data, and financial details, results in losses for the customers. Data breaches can occur due to cyberattacks, mishandling of data, or internal security breaches. Besides posing risks of identity theft, fraud, and financial abuse, the leakage of personal banking data erodes customers' trust in banking institutions and leads to significant reputation damage.²⁶

In general, customers face various security risks when using digital banking services, including cyber threats like phishing, malware, and denial of service (DoS) attacks. The digital services of Bank Syariah Indonesia (BSI) experienced disruptions or errors for several days on May 8, 2023. The disruption was caused by system maintenance and indications of a cyberattack. Customers complained about difficulties accessing services such as transactions through the BSI Mobile application, ATMs, and tellers. Bank Syariah Indonesia (BSI) has normalized its services, including on the ATM network and branch offices, and has collaborated with various parties to ensure the security of customer systems and funds. BSI claimed that banking services returned to normal on May 11, 2023, but social media reports contradicted this, stating that banking services were still unavailable even a week later. Shortly thereafter, there were allegations of data breaches by hackers targeting BSI.²⁷

This disruption underscores the importance of enhancing resilience against cyberattacks in digital banking services. The digital transformation of banking must be accompanied by readiness in information technology infrastructure, especially in maintaining the reliability and security of digital banking services. On May 16, 2023, BSI confirmed that customer data and funds remained secure despite the service disruption. The Financial Services Authority (OJK) urged BSI to ensure that services returned to normal after the incident and requested all financial institutions in the banking industry to strengthen their digital resilience. On May 18, 2023, the LockBit ransomware group claimed to have stolen 1.5 terabytes of data from BSI after failed ransom negotiations. This indicates that BSI experienced serious disruptions to its digital services that affected its customers.

According to the opening mandate of the 1945 Constitution, as stated in the fourth paragraph, the Government of the Republic of Indonesia has a constitutional responsibility to provide protection to all Indonesian citizens and their descendants and to enhance the welfare of the general public, promote national intelligence, and participate in maintaining order in the world based on the principles of independence, eternal peace, and social justice. In this age of technological advancement, particularly in information and communication, these national objectives must be realized through tangible protection, such as safeguarding the personal data of every individual or resident in Indonesia.²⁸

²⁶Fatmala Putri, D., & Ratna Sari, W. (2023). Analisis Perlindungan Nasabah Bsi Terhadap Kebocoran Data Dalam Menggunakan Digital Banking. *Jurnal Ilmiah Ekonomi Dan Manajemen*, 1(4), 173–181. <https://doi.org/10.61722/Jiem.V1i4.331>

²⁷Utami, N., S. R., & A. B. N. (2023). Reputational Risk Management Strategy At Indonesian Sharia Bank And Muamalat Indonesian Bank. *Balance: Journal Of Islamic Accounting*, 4(1).

²⁸Marcelliana, V., Zahra, S. M., Adzani, N. N., Massaid, H. N., Badriyyah, N., Benita, R., Sukarto, M., Fitriani, C. N., Alief, T., & Bayhaqi, R. (2023). Penerapan Perlindungan Konsumen Terhadap Nasabah Pt. Bank Syariah Indonesia Dalam

If privacy includes data protection, it is important to maintain the confidentiality and dignity of individual privacy. Data protection encourages freedom in politics, religion, and personal activities. The ability to control one's destiny, the freedom to express oneself, and the privacy of personal life are a series of essential rights inherent in every living being, especially humans. Violations of personal information use still occur in Indonesia. For example, in the banking sector, there is the exchange of personal data through sharing systems among card center institutions, where customer data is exchanged. This information, including credit card transactions, can be disclosed or traded to third parties by banks, individuals, or companies collecting data.

Every person, whether alone or in groups with others, is guaranteed to be a consumer of certain products and/or services. In this situation, there are often weaknesses experienced by consumers, leaving them in an "unsafe" position given the weaker position of consumers compared to businesses, which are relatively stronger in some aspects. Therefore, consumers require universal legal protection.²⁹

Hadjon explains legal protection as protecting quality and standards, while recognizing human rights according to legal rules as a set of regulations that can protect something. In this case, bank customers, as consumers, have their interests protected by law against violations. Efforts to combat technology-based banking crimes are a global responsibility, as evidenced by UN General Assembly Resolution VIII/1990 on computer-related crimes, which urges member states to make more effective efforts to prevent computer misuse.³⁰

As information technology advances rapidly, so do the services issued by banks through the internet network. Regarding security, it is not only for the benefit of customers but also for the benefit of both parties, namely customers and banks as providers of banking industry services as a whole. Protecting the interests of consumers and the public when using financial institution services is the purpose of establishing the Financial Services Authority (OJK). The OJK institution has the authority to carry out its duties to supervise, inspect, investigate, protect consumers, and take other actions against financial service institutions, actors, and/or supporters of financial service activities as stipulated in the laws and regulations in the financial services sector.³¹

In the case of the data leak by Bank Syariah Indonesia's customers concerning consumer legal protection, customers can file complaints or report violations they experience to the relevant authorities, such as the Financial Services Authority (OJK) in Indonesia. OJK is responsible for overseeing banking activities, including sharia banks, and can take law enforcement actions against violations committed by bank parties. With consumer legal protection based on applicable regulations, it is hoped that Bank Syariah Indonesia's customers can feel safer and more protected when using digital banking services.

The problem of digital service disruptions in sharia banking due to hacker attacks involves very important aspects in the financial world, namely security and trust. As someone concerned about the progress of technology and its utilization in the financial sector, it is necessary to address this issue so that we can all become more aware of the risks of cyberattacks threatening the banking industry, including sharia banking. By understanding and addressing this issue, we can improve security infrastructure, provide better protection for customers, and ensure the reliability of sharia banking services.

Kasus Kebocoran Data Nasabah. Deposisi: *Jurnal Publikasi Ilmu Hukum*, 1(2), 180–194. <https://doi.org/10.59581/Deposisi.V1i2.562>

²⁹Celina Tri Siwi Kristiyanti. (2011). *Hukum Perlindungan Konsumen*. Bengkulu: Sinar Grafika.

³⁰Philipus M. Hadjon, Pengkajian Ilmu Hukum Dogmatik (Normatif), *Yuridika*: Vol. 8 No. 1 (1994): Volume 8 No 1 Januari 1994

³¹Nasser Atorf. (2022). Internet Banking Indonesia. *Jurnal Manajemen Teknologi*, 1(1).

In the case of the data leak of Bank Syariah Indonesia's customers, the stolen data includes names, phone numbers, addresses, account balances, account numbers, transaction histories, account opening dates, and job information. Ransomware stole customer data from BSI, including financial documents, legal documents, and passwords.

Based on interviews conducted by researchers with several victims of this data theft case, many consumers could not access BSI Mobile Banking Services and encountered errors during the cyberattack. When consumers attempted to file complaints with BSI, they were unable to do so effectively due to the large number of complaints from other consumers. The second victim revealed that in this data

Forms of accountability certainly cannot be separated from the principle of civil liability, namely³² :

1. Principle of Liability Based on Fault: A person can only be held accountable if there is an element of fault committed.
2. Presumption of Liability: The defendant is always presumed liable until they can prove their innocence. The burden of proof lies with the defendant. This is known as the burden of reverse proof. This principle emphasizes always being responsible for any culpable loss, thus exempting one from liability. Proof is the responsibility of the aggrieved party.
3. Presumption of Non-Liability: The presumption of not always being liable is only known within the scope of very limited consumer transactions, and such limitations are usually justifiable based on common sense.
4. Strict Liability Principle: The principle of strict liability is often equated with the principle of absolute liability, where liability is without fault and there are no exceptions.
5. Limitation of Liability Principle: This principle of liability limitation is highly detrimental to consumers if unilaterally determined by businesses..

Looking at POJK No. 6/POJK.07/2022 in relation to the case, PT Bank Syariah Indonesia (BSI) must be accountable for the mistakes made towards its customers. However, this accountability does not require proof of fault elements or removing the fault elements. If civil law recognizes loss, or what we often call unlawful acts, where the violation of others must be borne and adjudicated under the law.

The forms of compensation for unlawful acts (PMH) recognized in the law are as follows:

1. Nominal Compensation: If there is an unlawful act involving intention that does not cause tangible loss to the victim, then the victim can be awarded a certain amount of money based on justice.
2. Compensation: It is compensation in the form of payment to the victim for the actual loss suffered from an unlawful act.

Penalty Compensation: This compensation is greater than the amount of the loss. The amount of compensation is intended to be applied to severe or sadistic intentional cases. PT Bank Syariah Indonesia must compensate customers for the losses resulting from system damage, making it difficult for customers to transact. Compensation includes refunding money or replacing equivalent-value goods and/or services for the lost customer money. The provision of such compensation does not preclude the possibility of criminal prosecution based

³²Fransiska Novita Eleanor. (2023). Prinsip Tanggung Jawab Mutlak Pelaku Usaha Terhadap Ketentuan Pasal 27 UU No. 8 Tahun 1999 Tentang Perlindungan Konsumen. Diakses Dari 301578-Prinsip-Tanggung-Jawab-Mutlak-Pelaku-Usa-8fc7ea70.Pdf (Neliti.Com), Pada Tanggal 13 Juni

on further evidence of fault. However, if businesses can prove that the fault is solely that of the consumer, compensation will not apply. However, looking at the case where one of the causes of data leakage is the bank's fault, customers—in this case, the customers of PT Bank Syariah Indonesia—are entitled to compensation provided by the bank.

Viewed from the case of PT Bank Syariah Indonesia (BSI) against its customers who are suspected of hacking customer data from BSI and spreading by a group of LockBit hackers, resulting in financial transaction disruptions. This case, in our opinion, constitutes an unlawful act (PMH). As stated in Article 11 of the PUIK, it is not allowed to provide personal data or information about consumers to other parties. Personal data and/or information as referred to in paragraph (1) include individual data such as name, National Identification Number, address, date of birth and/or age, telephone number, mother's name, and/or other data submitted or given access by consumers to PUIK.

In this regard, if viewed in terms of unlawful acts, customers can demand compensation from PT Bank Syariah Indonesia (BSI) by filing a lawsuit through the District Court in accordance with POJK No. 6/POJK.07/2022, Article 11. Because in this case, the principle of strict liability directs that PT Bank Syariah Indonesia must be accountable for the leakage of customer data without the need for proof of fault. POJK No. 6/POJK.07/2022 also regulates the forms of sanctions and compensation for unlawful acts, such as administrative sanctions and fines. Article 51 of POJK No. 6/POJK.07/2022 also explains that consumers and the public can utilize the services provided by the Financial Services Authority in the form of information reception services, information provision services, and complaint services.

Based on Regulation No. 6/POJK.07/2022, created to protect consumers and the public in the financial services sector, these principles can be found in Article 2 in the form of appropriate instructive data, clarity and explanation of data, fair and attentive treatment in conducting activities, security of resources, protection, and data of buyers, and handling of complaints and questioning purposes with sincerity and professionalism. In line with this, Islamic banks in this POJK must guarantee the confidentiality of customer data and information. If there is a leakage of customer data, then the Sharia bank must be liable for the resulting losses, unless it can prove that the leakage is not due to the Sharia bank's fault.

The Financial Services Authority has previously issued Regulations on Consumer Protection for Financial Services, namely POJK Number 1/POJK.07/2013, which was then revised into POJK Number 6/POJK.07/2022. This latest POJK further strengthens regulations on consumer protection and fosters the obligation of financial service providers to face changes in the financial services sector. In POJK 2022, sufficient legal protection is provided for consumers, especially bank customers, as it substantiates protecting data or information and ensuring the security of information systems and cyber resilience. In Article 8, the accountability of PUIK for consumer losses is also fully explained, concerning all personal data and information of consumers. In Article 11, a prohibition is also included for PUIK to provide personal data or information about consumers to other parties. Regarding consumer complaint services in Article 42, there is dispute resolution in the financial services sector outside the courts conducted through the Financial Services Sector Dispute Resolution Agency (LAPS).

In the case of customer data leakage at BSI allegedly carried out by hackers, these principles indicate that BSI must provide compensation to affected customers. This case has caused losses to customers, so the bank is obliged to compensate for the damages according to the applicable regulations. Customers have the right to demand compensation through legal channels in accordance with the prevailing regulations, with the burden of proof lying on the problematic customers. With the rapid growth of the digital economy, protecting customers in the utilization of digital banking services becomes essential, and the implementation of legal protection and

effective security policies will be a crucial foundation for sustainability and customer trust in the digital economy era. Therefore, to achieve success in the digital economy, Shariah banks must tighten their protection of customer data.

CONCLUSION

Personal data refers to information about an individual that is identified or can be identified either independently or in combination with other information, whether directly or indirectly through electronic or non-electronic systems. Personal data is closely related to private information, as it reveals personal information about an individual. Banking institutions rely on the public's trust for their sustainability. Therefore, to maintain public trust in banks, the government must strive to protect the public as bank customers. The leakage of personal data of customers has legal provisions for consumer and public protection outlined in OJK Regulation No. 06/POJK.07/2022 concerning Legal Protection in the Financial Services Sector, aimed at strengthening consumer protection aspects, including the protection of bank customer personal data as financial service consumers, as stipulated in Article 1, paragraph 4. This regulation emphasizes the prohibition of providing consumers' personal data to third parties. Personal data and information that must be protected are outlined in the OJK Regulation. This regulation includes rules on legal sanctions for parties that fail to comply with the provisions, such as provisions regarding the prohibition for financial service providers to misuse consumers' personal data or information. Sanctions imposed include administrative sanctions and nominal fines.

The case of the leakage of data from Bank Syariah Indonesia's customers due to ransomware stealing BSI customer data in the form of financial documents, legal documents, and passwords, as well as illegal transactions in BSI's mobile banking not conducted by customers, in this case, consumers cannot proceed with legal action due to a lack of knowledge of the regulations set by the OJK. Efforts to provide legal protection for customers' personal data in banking services against cybercrimes in Bank Syariah Indonesia should be seen through the latest OJK regulations, and PT. Bank Syariah Indonesia must compensate customers for the damage caused by system malfunctions and unlawful acts (PMH). This is clearly stated in Article 11 regarding the prohibition of providing consumers' personal data and/or information. Bank Syariah Indonesia must be accountable for the leakage of customer data without the need for proof of fault because sanctions for data breaches are also regulated by law.

BIBLIOGRAPHY

Journal and Books:

- Abdurrazaq Triansyah, P. N. S. J. N. F. A. M. A. (2022). *Peran Otoritas Jasa Keuangan Dalam Perlindungan Hukum Bagi Pengguna Pinjaman Online Ilegal (Studi Kasus Pinjol Ilegal Di Yogyakarta)*. . 5(2).
- Alga Soraja, (2020) *Perlindungan Hukum Atas Hak Privasi Dan Data Pribadi Dalam Perspektif HAM*, Prosiding Seminar Nasional Kota Ramah Hak Asasi Manusia, Universitas 1 Agustus 1945 Surabaya
- Amatul Najla. (2023). *Perlindungan Hukum Terhadap Konsumen Pinjaman Berbasis Online Oleh Otoritas Jasa Keuangan (Ojk) Berdasarkan Pojk Nomor 6/Pojk.07/2022. Madani : Jurnal Ilmiah Multidisiplin*, 1(8).

- Anggitafani, R. F. (2021). Perlindungan Hukum Data Pribadi Peminjam Pinjaman Online Perspektif Pojk No. 1/Pojk.07/2013 Tentang Perlindungan Konsumen Sektor Keuangan Dan Aspek Kemaslahatan..*Journal Of Islamic Business Law*, 2(2).
- Benuf, (2019). Otoritas Jasa Keuangan Republik Indonesia. *Refleksi Hukum Jurnal Ilmu Hukum*, 3(2).
- Celina Tri Siwi Kristiyanti. (2011). *Hukum Perlindungan Konsumen*. Bengkulu: Sinar Grafika.
- Daniar Supriyadi. (2017) "Data Pribadi dan Dua Dasar Legalitas Pemanfaatannya". <https://www.hukumonline.com/berita/baca/lt59cb4b3feba88/data-pribadi-dan-dua-dasar-legalitaspemanfaatannya-oleh--daniar-supriyadi/>. Diakses pada 16 Maret 2020. Pukul 18.04 WIB
- Fadlia, D. H., & . Y. (2015). Peran Otoritas Jasa Keuangan (Ojk) Dalam Perlindungan Hukum Bagi Investor Atas Dugaan Investasi Fiktif. *Law Reform*, 11(2), 207. <https://doi.org/10.14710/Lr.V11i2.15768>
- Fajrin Putri Carolin. (2022). Analisis Pengaturan Perlindungan Data Pribadi Pengguna Fintech Lending Dalam Peraturan Ojk Nomor 06/Pojk.07/2022. *Jurnal Ilmiah Wahana Pendidikan*, 8(8).
- Fatmala Putri, D., & Ratna Sari, W. (2023). Analisis Perlindungan Nasabah Bsi Terhadap Kebocoran Data Dalam Menggunakan Digital Banking. *Jurnal Ilmiah Ekonomi Dan Manajemen*, 1(4), 173–181. <https://doi.org/10.61722/Jiem.V1i4.331>
- Fransiska Novita Eleanora. (2023). Prinsip Tanggung Jawab Mutlak Pelaku Usaha Terhadap Ketentuan Pasal 27 Uu No. 8 Tahun 1999 Tentang Perlindungan Konsumen. *Diakses Dari 301578-Prinsip-Tanggung-Jawab-Mutlak-Pelaku-Usa-8fc7ea70.Pdf (Neliti.Com), Pada Tanggal 13 Juni .*
- Gerhat Sinaga, G., Sulistiyanto Jusuf, A., Kornelius, Y., Desi, D., Tarina, Y., Hukum, F., Veteran, U. “, & Jakarta, “. (2023). *Analisis Peran Otoritas Jasa Keuangan Terhadap Perbankan Sebagai Upaya Perlindungan Data Pribadi Nasabah Bank (Studi Kasus Kebocoran Data Nasabah Bank Syariah Indonesia)*.
- Marcelliana, V., Zahra, S. M., Adzani, N. N., Massaid, H. N., Badriyyah, N., Benita, R., Sukarto, M., Fitriani, C. N., Alief, T., & Bayhaqi, R. (2023). Penerapan Perlindungan Konsumen Terhadap Nasabah Pt. Bank Syariah Indonesia Dalam Kasus Kebocoran Data Nasabah. *Deposisi: Jurnal Publikasi Ilmu Hukum*, 1(2), 180–194. <https://doi.org/10.59581/Deposisi.V1i2.562>
- Mirza Alvina Maharani (2022), Perlindungan Nasabah Bank Syariah BUMN Pasca Merger Ditinjau Berdasarkan Hukum Perseroan Terbatas dan Hukum Perbankan, *International Journal Of Sociology, Policy And Law (IJOSPL)* Vol. 3 No. 2
- Murdiyanto, E. (2020). Metode Penelitian Kualitatif (Sistematika Penelitian Kualitatif). In *Bandung: Rosda Karya* (Veteran Pr). [Http://www.Academia.Edu/Download/35360663/Metode_Penelitian_Kualitaif.Docx](http://www.Academia.Edu/Download/35360663/Metode_Penelitian_Kualitaif.Docx)
- Nasser Atorf. (2022). Internet Banking Indonesia. *Jurnal Manajemen Teknologi*, 1(1).
- Ni Made Intan Pranita Dewanthara, M. G. S. K. R. (2020). Perlindungan Hukum Terhadap Pihak Pemberi Pinjaman Akibat Terjadinya Gagal Bayar Peer To Peer Lending. . *Jurnal Hukum Kenotariatan Fakultas Hukum Universitas Udayana*, 5(3).

- Nursantih, N., & Ratnawati, E. (2023). *Pengawasan Ojk Atas Data Pribadi Konsumen Pada Perusahaan Peer To Peer Lending*. 5(4). <https://doi.org/10.31933/Unesrev.V5i4>
- Otoritas Jasa Keuangan. (2015). Otoritas Jasa Keuangan, Workshop Perlindungan Konsumen Di Sektor Jasa Keuangan, . *Bidang Edukasi Perlindungan: Jakarta*.
- Pamelia Herfesia Safsafubun. (2023). Analisis Perlindungan Konsumen Terhadap Transaksi Elektronik Pada Lembaga Perbankan Berdasarkan Peraturan No. 6/Pojk.07/2022. *Jimps: Jurnal Ilmiah Mahasiswa Pendidikan Sejarah*, 4(1).
- Peraturan Otoritas Jasa Keuangan Republik Indonesia. (2022). *Otoritas Jasa Keuangan Republik Indonesia Nomor 6 /Pojk.07/2022*.
- Philip Alston, (2008) Hukum hak asasi manusia, PUSHAM UII: Yogyakarta.
- Philippus M. Hadjon, Pengkajian Ilmu Hukum Dogmatik (Normatif) , Yuridika: Vol. 8 No. 1 (1994): Volume 8 No 1 Januari 1994
- Putri Annisya Chaerani. (2023). Perlindungan Hukum Konsumen Atas Penyalahgunaan Data Pribadi Oleh Perusahaan Fintech Dalam Transaksi Peer To Peer Lending. *Jurnal Ilmiah*.
- Saleh, Hm., Febryan Fitrahady, K., Zuhairi, A., Sutrisno, B., & Annisya Chaerani, P. (2023). *Penyuluhan Tentang Penanganan Penyalahgunaan Data Pribadi Terhadap Nasabah Peer To Peer Lending Berdasarkan Hukum Positif Di Kecamatan Gunung Sari (Vol. 5)*.
- Sekretariat Kabinet Republik Indonesia. (2023). Ojk Terbitkan Aturan Baru Perlindungan Konsumen. <https://setkab.go.id/ojk-terbitkan-aturan-baru-perlindungan-konsumen>.
- Syukron. (2019). Pengantar Sistem Hukum Asuransi Syariah Dan Kepailitan Di Indonesia. *Indramayu: Adab*, 3(2).
- Utami, N. , S. R. , & A. B. N. (2023). Reputational Risk Management Strategy At Indonesian Sharia Bank And Muamalat Indonesian Bank. . *Balance: Journal Of Islamic Accounting*, 4(1).
- Wardah Yuspin. (2023). Penerapan Kebijakan Countercyclical Terhadap Fintech Syariah Peer To Peer Lending: Studi Kasus Pt. Alami Fintek Sharia Dan Pt. Investree Radhika Jaya. *Jurnal Hukum Magnum Opus*, 6(1).
- Wijaya, Hengki, Umriati. (2020). *Analisis Data Kualitatif*. Sekolah Tinggi Theologia Jaffray.