M. Bintang Faqih Khudori "Analysis of Customer Protection against Personal Data Abuse by Banks in Indonesia: A Case Study of Shari'ah Banks in Indonesia" *Varia Hukum: Jurnal Forum Studi Hukum dan Kemasyarakatan* 7 no. 1 (2025): 39-54. DOI: 10.15294/vhv7i1.41656

Varia Hukum

Jurnal Forum Studi Hukum dan Kemasyarakatan
Volume 7 Issue 1, 39-54, June 2025
P-ISSN: 2085-2254, E-ISSN: 2798-7663

Analysis of Customer Protection against Personal Data Abuse by Banks in Indonesia: A Case Study of Shari'ah Banks in Indonesia

M. Bintang Faqih Khudori

[1] *State Islamic Univeristy of Sunan Gunung Djati Bandung, Indonesia. E-mail: bintangfaqih514@gmail.com*

Abstract: Protection of customer personal data in the Indonesian banking sector is increasingly becoming a major concern with the rapid development of digital technology. The shift of banking transactions to digital platforms increases the risk of data leaks and the threat of cyber-attacks, requiring stricter regulations to safeguard sensitive customer information. This article evaluates the effectiveness of personal data protection regulations, including the implementation of the recently enacted Personal Data Protection Law, which in Indonesian, is named *Undang-Undang Perlindungan Data Pribadi* (UU PDP), as well as banks' responsibilities in maintaining the confidentiality and security of customer data. Using a normative juridical approach, this research assesses the policies and implementation of data protection by banks in Indonesia. The results of the analysis show that although many banks have taken proactive steps to protect customer data, there are still significant challenges in implementing regulations and increasing public awareness. Therefore, additional measures are needed to strengthen personal data protection and increase customer confidence in the banking system.

Keywords: Personal Data Protection, Banking Regulation, Cyber Security

1. Introduction

In this digital era, technology is used in all aspects of human life, one of the aspect is in the banking sector in Indonesia. Banking transactions that were previously done manually have moved now to digital platforms such as internet banking, mobile banking, and various other financial services applications.[1] These changes certainly bring benefits in terms of effectiveness

[1] Rifany Aprilia Hernanda, *Perlindungan Hukum Data Pribadi Nasabah Bank Digital Pada Sektor Perbankan Di Indonesia* (Universitas Sebelas Maret, 2022), https://digilib.uns.ac.id/dokumen

**Correspondence*
Article Info [Submitted: 10 April 2025 | Revised Version 10 June 2025 | Accepted: 30 June 2025]

and convenience for customers, but also pose new risks related to data security. When customer data, including personal and financial information, is processed and stored in digital systems, the threat of data leakage or cyber attacks becomes more significant. Therefore, customer data protection is crucial to ensure that sensitive data remains protected and secure from unauthorised access.[2]

Along with the development of technology, cybersecurity threats are also increasingly complex and diverse. Cybercriminals continue to develop new methods to exploit loopholes in banking security systems. Attacks such as phishing, malware, and hacking can lead to customer data leaks that have the potential to cause financial losses and damage the bank's reputation. Several high-profile cases of data breaches have shown how important it is to protect customer data. In this context, banking law plays an important role in setting strict standards and regulations to protect customer data from cybersecurity threats.[3]

Bank customers have the right to feel safe and comfortable using banking services. The protection of customer data is part of the protection of consumer rights governed by various regulations and international standards. The Personal Data Protection Law (UUPDP) implemented in many countries aims to protect the privacy and security of individual data. In Indonesia, the Personal Data Protection Bill is also being discussed to provide a stronger legal umbrella for the protection of personal data, including bank customer data. Customer data protection also includes the right to know how their data is collected, stored and used, as well as the right to request data deletion if necessary.[4]

/detail/90345/Perlindungan-Hukum-Data-Pribadi-Nasabah-Bank-Digital-Pada-Sektor-Perbankan-Di-Indonesia.

2 "Peraturan Bank Indonesia No. 7/6/PBI/2005 Tentang Transparansi Informasi Produk Bank Dan Penggunaan Data Pribadi Nasabah.," 2005, https://sarolangunkab.go.id/artikel/baca/poin-penting-dalam-ruu-perlindungan-data-pribadi.

3 Diana Setiawati, Tyas Permata Dewi, and Zulfiana Ayu Astutik, "Personal Data Protection Vulnerabilities In Cybercrime Sniffing Bank Account Break-Ins," *Yurispruden: Jurnal Fakultas Hukum Universitas Islam Malang* 7, no. 2 (2024): 184–99, https://doi.org/10.33474/yur.v7i2.21184.

4 "Undang-Undang No. 27 Tahun 2022 Tentang Perlindungan Data Pribadi," 2022.

Banks have a legal responsibility to protect the confidentiality and security of customer data. This obligation is set out in various banking regulations, such as Law No. 10 of 1998 on Banking, as well as regulations issued by the *Otoritas Jasa Keuangan*(OJK), which is Financial Services Authority.[5] This obligation includes the implementation of adequate security measures, regular audits, as well as the reporting of data leakage incidents. Banks are also required to provide training and awareness raising to employees on the importance of customer data protection. Failure to fulfil these obligations may result in legal sanctions, including fines and revocation of operating licences.

Customer trust is an important asset for banks. Leaked customer data can undermine that trust and significantly harm the bank's reputation. Customers who feel that their personal data is not secure may choose to switch to another bank that is considered more secure. Therefore, protecting customer data is also an effort to maintain the trust and reputation of the bank. Banks that successfully protect customer data are more likely to be trusted and respected by customers, which in turn can increase customer loyalty and overall business performance.[6]

In the era of globalisation, banks not only operate domestically but also engage in international transactions and services. This requires banks to comply with international standards and regulations regarding data protection. International conventions such as the General Data Protection Regulation (GDPR) in the European Union set high standards for data protection that companies, including banks, operating in the region or handling data of EU citizens must comply with. Compliance with these international standards is important to ensure banks can compete globally and avoid sanctions from international authorities.

For example, headline-grabbing leaks of customer data at certain banks have highlighted gaps in banks' security systems and weak oversight. In addition,

---

5 Otoritas Jasa Keuangan, "Pedoman Keamanan Data Dan Informasi Perbankan.," 2021.

6 Selvina Nur Amalia, *Analisis Perlindungan Data Pribadi Nasabah Pada Bank Syariah Mandiri Terhadap Regulasi*, vol. 4, 2016, https://repository.uinjkt.ac.id/dspace/bitstream/123456789/42471/1/Selvina Nur Amalia-FSH.pdf.

with the development of digital banking services, threats to data security are increasingly complex, including risks from cyber-attacks and internal abuse. Therefore, the protection of customer data is not only a legal issue, but also an issue of public trust in the banking system.

Personal data is a very important component in the digital era, especially when almost every human activity is connected to technology, whether through financial transactions, app usage, or other digital-based services. In the context of Indonesian law, the definition of personal data has been clearly regulated in Article 1 paragraph (1) of Law Number 27 Year 2022 on Personal Data Protection (PDP Law), which states that personal data is:

> '*data about a person that can be identified alone or combined with other information either directly or indirectly through electronic and non-electronic systems.*'[7]

From the above definition, there are two emphases that can be concluded. First, directly identifiable data, which is data that directly shows a person's identity, such as name, identity number (KTP, passport), date of birth, address, and telephone number. This information is usually the basic requirement collected by banks for opening accounts or applying for financial products. Second, indirectly identifiable data, which is data that requires further processing to identify individuals, such as financial transaction data, location history, shopping preferences, or digital information such as IP addresses, browser cookies, and biometric data (fingerprints, facial recognition, voice). This kind of data is often the target of abuse in data breach cases, as it has a high value to cyber criminals. In the context of banking, personal data includes all information relating to the customer, including identity data and financial information. Personal data protection is important as this data is sensitive and can be used for unauthorised purposes if not properly protected. In the banking sector, personal data is often considered a

[7] Wulan Rannie B., "Legal Protection of Customer Personal Data in the Banking Sector," *ARRUS Journal of Social Sciences and Humanities* 3, no. 5 (2023): 710–17, https://doi.org/10.35877/soshum2169.

bank secret, which means that the bank has an obligation to keep the data confidential.[8]

The Personal Data Protection Law (PDP Law) promulgated through Law No. 27 of 2022 is an important regulation that serves as the legal basis for personal data protection in Indonesia. This regulation regulates the rights, obligations, and sanctions associated with the management of personal data, including in the banking sector which has a very large volume of customer data.

Firstly, the rights of data owners. The PDP Law provides protection to customers as data owners by establishing a number of key rights. Based on Article 5 of the PDP Law, customers have the right to obtain information about the purpose of collecting, using, and processing their personal data. In the banking sector, this information is usually provided in the customer's consent document when opening an account or using bank services, including digital services such as mobile banking. Based on Article 9 of the PDP Law, customers have the right to revoke their consent to the processing of personal data by banks, especially if the data is used for purposes that are not in accordance with the initial agreement, such as direct marketing without the customer's permission. Finally, based on Article 14 of UU PDP, customers can request the deletion or destruction of data that is irrelevant or no longer needed by the bank. For example, if the customer has closed their account, the data related to the account must be deleted, except for data that is required to be kept for a certain period of time by other regulations, such as the Banking Law.[9]

Secondly, the obligations of the data controller (Bank). Banks as data controllers have a great responsibility in maintaining the confidentiality, security, and integrity of customer data. Some of the obligations stipulated in the PDP Law are: First, the Bank must maintain the confidentiality of

---

[8] Anvesh Gunuganti, "Problems of Personal Data Protection in the Digital Age," *Journal of Scientific and Engineering Research* 5, no. 12 (July 11, 2018): 358–65, https://doi.org/10.34925/EIP.2022.141.4.051.

[9] Elsam, "Perlindungan Data Pribadi Usulan Pelembagaan Kebijakan Dari Perspektif Hak Asasi Manusia.," 2016, https://perpustakaan.elsam.or.id/index.php?p=show_detail&id=15096&keywords=.

customer personal data and take adequate technical and organisational measures to prevent data leakage. In the event of data leakage, banks are obliged to report it to the authorities within a maximum of 72 hours from the time the incident is noticed. Furthermore, the Bank may only use the customer's personal data for agreed purposes, such as for administrative purposes or financial services. The use of data for other purposes, such as marketing third-party products, must obtain additional consent from the customer.[10]

Customer data protection is an important aspect of the relationship between banks and customers, as clearly regulated in Article 40 of Law No. 10 of 1998 on Banking. This regulation makes customer data security an integral part of the principle of bank secrecy, with the aim of maintaining customer trust and supporting the stability of the banking sector in Indonesia.

Article 40 of the Banking Law explicitly states that banks are obliged to maintain the confidentiality of information about customers and their deposits. This information includes Customer Identity, Financial Transaction Information, Information related to Account Balances, Loans, or Other Data Considered Confidential. This confidentiality aims to protect customers from the risk of data misuse, such as identity theft, fraud, or unauthorised access by third parties. Customer data security is one of the important aspects in maintaining customer trust in the bank.[11]

Although the principle of confidentiality applies strictly, Article 40 also regulates exceptions to confidentiality under certain conditions, among others, for Tax Purposes, banks are obliged to provide information related to customers to the Directorate General of Taxes if requested. This exception aims to support supervision and law enforcement in the taxation sector. For Criminal Investigation Purposes, customer information may be disclosed at the request of law enforcement agencies in the process of investigation or prosecution of criminal cases. This is important to support law enforcement

---

[10] Hukum Online, "Memahami Persetujuan Data Pribadi Di Sektor Perbankan Indonesia.," hukumonline.com, 2023.

[11] "Undang-Undang No. 10 Tahun 1998 Tentang Perubahan Atas Undang-Undang No. 7 Tahun 1992 Tentang Perbankan," 1998.

efforts and eradicate criminal offences. Upon Court Order, customer information may be provided to certain parties pursuant to a court order. This exception is made to fulfil a court decision in the context of resolving a dispute or legal case.

If the bank violates the confidentiality provisions of customer data, there are several legal consequences that can be applied, namely: 1) Administrative Sanctions, the Financial Services Authority (OJK) can give a written warning to banks that violate confidentiality provisions. In cases of violations that are considered serious, OJK has the authority to suspend or revoke the bank's business licence.[12] 2) Criminal Sanctions, Violation of bank secrecy is punishable by imprisonment for a maximum of 4 years and/or a maximum fine of IDR 8 billion, as stipulated in Article 47 of the Banking Law. These criminal sanctions aim to provide a deterrent effect and ensure that banks comply with existing confidentiality provisions.

2. Methods

This research applies an analytical descriptive method with a normative juridical approach to explore the protection of customer personal data in the banking sector in Indonesia. The analytical descriptive method is used to describe and explain the object of research by collecting relevant data and examples, without attempting to draw general conclusions.

Meanwhile, the normative juridical approach is conducted through the study of library materials, which are secondary data, also known as library legal research. In this approach, researchers conducted an inventory of positive laws, including applicable laws and regulations and draft regulations, as well as relevant local government policies.

The results of this research are then linked to the views and findings from other studies to provide a more comprehensive understanding of the

[12] Raissa Avila Nasution et al., "Perlindungan Hukum Terhadap Data Pribadi Nasabah Layanan Perbankan Setelah Berlakunya Peraturan Otoritas Jasa Keuangan (POJK) Nomor 6/Pojk.O7/2022," *Journal of Education, Humaniora and Social Sciences (JEHSS)* 7, no. 1 (August 10, 2024): 71–78, https://doi.org/10.34007/jehss.v7i1.2292.

challenges and effectiveness of customer personal data protection regulations in Indonesian banks.

3. Results and Discussion

3.1 Policy and Implementation of Personal Data Protection at Banks in Indonesia

In Indonesia, personal data protection is governed through various policies and regulations designed to protect individual privacy and data security. One of the main regulations is Law No. 27 of 2022 on Personal Data Protection (PDP Law), which regulates the rights of data owners, including the right to access, correct, and delete their personal data. In addition, the PDP Law also regulates the obligations of data controllers to protect the data they manage and sets sanctions for violations that occur. With the PDP Law, Indonesia seeks to raise the bar for personal data protection and put itself on par with other countries that already have similar regulations in place.[13]

Alongside the PDP Law, Law No. 10 of 1998 on Banking also plays an important role in the protection of personal data, particularly in the context of financial institutions. This law requires banks to maintain the confidentiality and security of their customers' data. This includes sensitive information relating to financial transactions and customer identity. The Financial Services Authority (OJK) as the supervisor of the financial sector also issues regulations that ensure that banks comply with personal data protection provisions, thus providing an additional layer of protection for consumers.[14]

The implementation of personal data protection policies in Indonesian banks shows significant variation. Many banks have taken proactive steps to protect customer data by adopting various security technologies, such as data encryption, intrusion detection systems, and regular security audits. These

---

[13] Kadek Rima Anggen Suari and I Made Sarjana, "Menjaga Privasi Di Era Digital: Perlindungan Data Pribadi Di Indonesia," *Jurnal Analisis Hukum* 6, no. 1 (April 25, 2023): 132–42, https://doi.org/10.38043/jah.v6i1.4484.

[14] Dewan Perwakilan Rakyat, "Undang-Undang Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi," 2022.

measures aim to prevent unauthorised access and maintain the confidentiality of customer information. In addition, training and raising employee awareness on the importance of data protection is also a key focus, with the aim of ensuring that all staff understand their responsibilities in safeguarding customers' personal data.[15]

3.2 Cases of Personal Data Misuse and its Impact on Customers

Various cases of personal data misuse by banks in Indonesia have certainly caused excessive concern for customers, with some striking cases showing the vulnerability of data security systems. One of the most significant examples is the data breach incident involving Bank Syariah Indonesia (BSI), where the hacker group Lockbit 3.0 managed to steal approximately 1.5 terabytes of sensitive data. The stolen data included personal information of 15 million customers, including names, addresses, phone numbers, account balances and transaction history. This leak not only threatened the privacy of individuals but also damaged the reputation of banks, causing many customers to lose trust in the services they use.

The impact of this data leak is far-reaching. Affected customers are at risk of identity fraud and misuse of their personal information. In some cases, the leaked information may be used by third parties to commit financial fraud, such as opening new accounts or applying for loans using someone else's identity.[16] In addition, these leaks can cause direct financial losses to customers, as well as additional costs to rectify problems caused by identity theft.

Banks that experience data breaches also face legal consequences. The Financial Services Authority (OJK) can sanction banks that are found to be negligent in protecting their customers' data. Such sanctions could include fines or even revocation of operating licences for banks that fail to meet data protection standards. This emphasises the importance of compliance with

---

[15] Willa Wahyuni, "Bank Perlu Edukasi Nasabah Terkait Pelindungan Data Pribadi," Hukumonline.com, 2022.

[16] Moh Khory Alfarizy, "15 Juta Data Nasabah BSI Diduga Bocor, Pakar Siber: Hati-Hati Serangan Phising Ke Pemilik Rekening," Tempo.co, 2018.

personal data protection regulations and the need to invest in better security technologies to protect sensitive information.

In addition, data breach incidents can cause long-term impacts on the relationship between banks and customers. Trust is a key factor in banking relationships; when this trust is shaken due to a data breach, customers may choose to withdraw their funds or switch to other financial institutions. This can affect the stability of banks and lower their market share in the banking industry.

Data leaks have also raised concerns among the general public about the security of their personal information. Many people have become more aware of the potential risks of data misuse and have started looking for ways to protect themselves. Data security education is important so that customers can recognise the signs of potential fraud and take steps to protect their personal information.[17]

3.3 Analysis of Regulatory Compliance with Personal Data Protection Principles

Regulatory conformity with personal data protection principles in Indonesia, particularly through the Personal Data Protection Law (PDP Law), demonstrates significant efforts to protect the rights of individuals. The PDP Law was drafted to provide a solid legal basis for personal data management, covering the rights of data subjects, such as the right to access, correct, and delete their personal data. This is in line with international data protection principles that emphasise transparency, accountability, and consent from data owners before their information is processed.[18] With the PDP Law, Indonesia endeavours to create a comprehensive legal framework that not only protects individuals but also provides legal certainty for businesses in the management of personal data.

---

[17] Trianda Lestari, Syahrando Muhti, and Reky Yuliansyah, "Pertanggungjawaban Perbankan Dalam Melindungi Data Pribadi Nasabah Akibat Peretasan Studi Kasus Bank Syariah Indonesia," *Doktrin: Jurnal Dunia Ilmu Hukum Dan Politik* 2, no. 3 (May 17, 2024): 48–59, https://doi.org/10.59581/doktrin.v2i3.3202.

[18] Henri Subiakto, *Perlindungan Data Pribadi dan Tantangannya*, 2021.

However, while the PDP Law demonstrates compatibility with the principles of personal data protection, challenges in its implementation remain. One of the main challenges is the public's low awareness of their rights regarding data protection. Many individuals still do not understand the importance of data privacy and how to protect their personal information. This can lead to non-compliance with regulations and increase the risk of misuse of personal data. In addition, while there are many regulations governing data protection in Indonesia, there is no single comprehensive legal umbrella that effectively integrates all aspects of data protection.

Other challenges in implementing the PDP Law are the difference understanding and application of regulations across sectors. For example, the public and private sectors may have different standards in protecting personal data. Some agencies may not have adequate resources or infrastructure to comply with regulatory requirements.[19] Thus, synergy between the government, law enforcement agencies, and the private sector is needed to ensure compliance and understanding of the regulations by all parties.

Improving effectiveness of personal data protection regulations in Indonesia, is important to socialise and educate the public on their privacy rights. The government and relevant agencies need to organise information campaigns that explain the importance of personal data protection as well as the steps that individuals can take to protect their information. By increasing public awareness, a positive behavioural change towards personal data management is expected.[20]

In addition, supervision and law enforcement should also be strengthened to ensure that violations of the PDP Law are followed up with appropriate sanctions. The Financial Services Authority (OJK) and other relevant institutions need to have sufficient capacity to conduct audits and examinations of the compliance of banks and other financial institutions in

---

[19] Super Admin, "Poin Penting Dalam RUU Perlindungan Data Pribadi," Pemerintah Kabupaten Sarolangun, 2022, https://sarolangunkab.go.id/artikel/baca/poin-penting-dalam-ruu-perlindungan-data-pribadi.

[20] Winastwan Gora Swajati, "Strategi Implementasi Regulasi Perlindungan Data Pribadi Di Indonesia," *Indonesiana*, 2019, 1–26.

protecting customer data. Thus, public trust in the banking system and personal data management can be maintained.[21]

Overall, although the PDP Law has demonstrated conformity with the principles of personal data protection, challenges in its implementation still require serious attention. Through collaborative efforts between all stakeholders and increased public awareness, it is hoped that this regulation can be effectively implemented and provide optimal protection for the people of Indonesia.

3.4 Steps the Bank Can Take to Tighten Supervision

One of the key steps that banks can take is the implementation of strict information security policies. This includes the implementation of international standards such as ISO 27001, which helps banks in maintaining the confidentiality and integrity of customer data. This policy should include the use of strong passwords, multifactor authentication, and restricting access to information systems to only those employees who require such access. In addition, banks need to have effective monitoring systems in place to detect suspicious activities as well as conduct regular security audits to identify and fix vulnerabilities in their systems.[22]

In addition, comprehensive risk management is also very important. Banks should actively identify, evaluate, and manage the various risks associated with their operations, including cybersecurity risk, operational risk, and regulatory compliance risk. The use of a holistic approach in stress testing can help banks understand how they would fare under various crisis scenarios. Through such scenario-based performance projections, banks can prepare better strategic plans to face future challenges.[23]

---

21 "Undang-Undang No. 27 Tahun 2022 Tentang Perlindungan Data Pribadi."

22 Ferozi Ramdana Irsyad et al., "Menghadapi Era Baru : Strategi Perbankan Dalam Menghadapi Perubahan Pasar Dan Teknologi Di Indonesia," *Transformasi: Journal of Economics and Business Management* 3, no. 2 (2024): 29–46, https://doi.org/10.56444/transformasi.v3i2.1594.

23 Haris Firmansyah, "Cara Meningkatkan Pengawasan Risiko Di Bank: Panduan Tiga Langkah," Indonesia Risk Management, 2023.

Employee training is also an integral part of these surveillance measures. Banks should ensure that all employees understand the importance of information security and are trained to recognise and respond to potential threats such as phishing attacks. Building a culture of cybersecurity throughout the organisation will strengthen the bank's defences against cyberattacks.[24]

In the context of collaboration with external parties, banks need to establish partnerships with information security agencies and regulators such as the Financial Services Authority (OJK). This cooperation not only strengthens the bank's ability to deal with digital threats but also ensures that the technological innovations implemented remain in accordance with existing regulations.

4. Conclusion

From the analysis conducted, it can be concluded that the protection of customer personal data in Indonesian banking still faces various challenges despite the existence of a clear legal framework through the PDP Law and other related regulations. While some banks have shown strong commitment by implementing adequate security measures, there is uneven implementation of data protection policies across the banking sector. Factors such as limited resources and lack of understanding of the regulations hinder some banks from fulfilling their obligations. In addition, the effectiveness of supervision by the Financial Services Authority (OJK) is also affected by the ability of individual banks to implement data protection policies. Therefore, to improve personal data protection, it is recommended that OJK strengthen supervision and provide support to banks in terms of training and implementation of security technology. In addition, educating the public on their rights regarding data protection is also very important to build awareness and trust in the banking system in Indonesia. With these measures, it is expected that the protection of customers' personal data can be significantly improved, creating a safer and more trusted banking environment.

[24] Sandy Romualdus, "Strategi Penerapan Keamanan Siber Di Perbankan," Stabilitas.com, 2023.

References

Amalia, Selvina Nur. *Analisis Perlindungan Data Pribadi Nasabah Pada Bank Syariah Mandiri Terhadap Regulasi*. Vol. 4, 2016. https://repository.uinjkt.ac.id/dspace/bitstream/123456789/42471/1/Selvina Nur Amalia-FSH.pdf.

Anggen Suari, Kadek Rima, and I Made Sarjana. "Menjaga Privasi Di Era Digital: Perlindungan Data Pribadi Di Indonesia." *Jurnal Analisis Hukum* 6, no. 1 (April 25, 2023): 132–42. https://doi.org/10.38043/jah.v6i1.4484.

Dewan Perwakilan Rakyat. "Undang-Undang Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi," 2022.

Elsam. "Perlindungan Data Pribadi Usulan Pelembagaan Kebijakan Dari Perspektif Hak Asasi Manusia.," 2016. https://perpustakaan.elsam.or.id/index.php?p=show_detail&id=15096&keywords=.

Ferozi Ramdana Irsyad, Filja Azkiah Siregar, Jonatan Marbun, and Hasyim Hasyim. "Menghadapi Era Baru : Strategi Perbankan Dalam Menghadapi Perubahan Pasar Dan Teknologi Di Indonesia." *Transformasi: Journal of Economics and Business Management* 3, no. 2 (2024): 29–46. https://doi.org/10.56444/transformasi.v3i2.1594.

Gunuganti, Anvesh. "Problems of Personal Data Protection in the Digital Age." *Journal of Scientific and Engineering Research* 5, no. 12 (July 11, 2018): 358–65. https://doi.org/10.34925/EIP.2022.141.4.051.

Haris Firmansyah. "Cara Meningkatkan Pengawasan Risiko Di Bank: Panduan Tiga Langkah." Indonesia Risk Management, 2023.

Henri Subiakto. *Perlindungan Data Pribadi Dan Tantangannya*, 2021.

Hernanda, Rifany Aprilia. *Perlindungan Hukum Data Pribadi Nasabah Bank Digital Pada Sektor Perbankan Di Indonesia*. Universitas Sebelas Maret, 2022. https://digilib.uns.ac.id/dokumen/detail/90345/Perlindungan-Hukum-Data-Pribadi-Nasabah-Bank-Digital-Pada-Sektor-Perbankan-Di-Indonesia.

Moh Khory Alfarizy. "15 Juta Data Nasabah BSI Diduga Bocor, Pakar Siber: Hati-Hati Serangan Phising Ke Pemilik Rekening." Tempo.co,

2018.

Nasution, Raissa Avila, Budiman Ginting, Mahmul Siregar, and Tengku Keizerina Devi Azwar. "Perlindungan Hukum Terhadap Data Pribadi Nasabah Layanan Perbankan Setelah Berlakunya Peraturan Otoritas Jasa Keuangan (POJK) Nomor 6/Pojk.O7/2022." *Journal of Education, Humaniora and Social Sciences (JEHSS)* 7, no. 1 (August 10, 2024): 71–78. https://doi.org/10.34007/jehss.v7i1.2292.

Online, Hukum. "Memahami Persetujuan Data Pribadi Di Sektor Perbankan Indonesia." hukumonline.com, 2023.

Otoritas Jasa Keuangan. "Pedoman Keamanan Data Dan Informasi Perbankan.," 2021.

"Peraturan Bank Indonesia No. 7/6/PBI/2005 Tentang Transparansi Informasi Produk Bank Dan Penggunaan Data Pribadi Nasabah.," 2005. https://sarolangunkab.go.id/artikel/baca/poin-penting-dalam-ruu-perlindungan-data-pribadi.

Rannie B., Wulan. "Legal Protection of Customer Personal Data in the Banking Sector." *ARRUS Journal of Social Sciences and Humanities* 3, no. 5 (2023): 710–17. https://doi.org/10.35877/soshum2169.

Sandy Romualdus. "Strategi Penerapan Keamanan Siber Di Perbankan." Stabilitas.com, 2023.

Setiawati, Diana, Tyas Permata Dewi, and Zulfiana Ayu Astutik. "Personal Data Protection Vulnerabilities In Cybercrime Sniffing Bank Account Break-Ins." *Yurispruden: Jurnal Fakultas Hukum Universitas Islam Malang* 7, no. 2 (2024): 184–99. https://doi.org/10.33474/yur.v7i2.21184.

Super Admin. "Poin Penting Dalam RUU Perlindungan Data Pribadi." Pemerintah Kabupaten Sarolangun, 2022. https://sarolangunkab.go.id/artikel/baca/poin-penting-dalam-ruu-perlindungan-data-pribadi.

Swajati, Winastwan Gora. "Strategi Implementasi Regulasi Perlindungan Data Pribadi Di Indonesia." *Indonesiana*, 2019, 1–26.

Trianda Lestari, Syahrando Muhti, and Reky Yuliansyah. "Pertanggungjawaban Perbankan Dalam Melindungi Data Pribadi

Nasabah Akibat Peretasan Studi Kasus Bank Syariah Indonesia." *Doktrin: Jurnal Dunia Ilmu Hukum Dan Politik* 2, no. 3 (May 17, 2024): 48–59. https://doi.org/10.59581/doktrin.v2i3.3202.

"Undang-Undang No. 10 Tahun 1998 Tentang Perubahan Atas Undang-Undang No. 7 Tahun 1992 Tentang Perbankan," 1998.

"Undang-Undang No. 27 Tahun 2022 Tentang Perlindungan Data Pribadi," 2022.

Willa Wahyuni. "Bank Perlu Edukasi Nasabah Terkait Pelindungan Data Pribadi." Hukumonline.com, 2022.