


# The Urgency of Customer Personal Data Protection in Digital Banking

Alvin Hamzah Nasution

University of Medan Area, Indonesia; alvinhamzahnst@gmail.com

ARTICLE INFO	ABSTRACT
<p><b>Keywords</b></p> <p>Personal Data Protection; Legal Protection; Customer</p>	<p>The development of digital technology in the financial sector has transformed banking services to be more open, fast, and data-driven. On the other hand, the increasing intensity of processing customers' personal data also poses new challenges related to the protection of privacy rights. This study aims to examine the urgency of legal protection for customers' personal data in Indonesia's digital financial ecosystem. The method used is a normative legal approach with an analysis of regulations such as Law Number 27 of 2022 concerning Personal Data Protection and POJK No. 6/POJK.07/2022. The results of the study show that although Indonesia already has a formal legal framework, its implementation still faces obstacles such as the absence of a data supervisory authority, low digital legal literacy among the public, and weak enforcement of sanctions. Therefore, a holistic approach is needed in the form of strengthening regulations, public education, and harmonization with international standards to guarantee customer rights and build a safe and sustainable digital financial industry.</p>
<p><b>Article history:</b></p> <p>Received 2025-04-24 Revised 2025-05-22 Accepted 2025-06-30</p>	
<p><b>Corresponding Author:</b> Alvin Hamzah Nasution University of Medan Area, Indonesia; alvinhamzahnst@gmail.com</p>	<p><i>This is an open access article under the <a href="#">CC BY-NC</a> license.</i></p> 

## 1. INTRODUCTION

The development of digital technology has brought significant changes in the banking sector, where conventional services are now transforming into digital-based services to improve efficiency, convenience, and service reach to customers. However, this progress is also accompanied by challenges that are no less significant, one of which is the increasing risk to the security of customers' personal data. Important data such as identity, financial information, and transaction history stored in the digital banking system are very vulnerable to leakage or misuse if not supported by a reliable security system.(Maisah et al., 2023)

Various cases of customer personal data breaches that have occurred in Indonesia indicate that the data protection system in the banking world is still inadequate. Practices such as sending data to third parties without permission, identity theft, and using customer contact information for promotions without consent are evidence of the weak implementation of data protection principles as stipulated in Law Number 27 of 2022 concerning Personal Data Protection. This not only reflects the lack of technical protection, but also weak law enforcement and coordination between institutions, such as the OJK and the Ministry of Communication and Informatics.(Denisya et al., 2024)

In fact, maintaining the confidentiality of personal data is not only important as a form of fulfilling the individual's right to privacy guaranteed by the constitution, but also a major pillar in building public trust in banking institutions. This trust is the main foundation of the modern banking system. If customer data is not managed safely, transparently, and accountably, the reputation of financial institutions can be threatened, even impacting the stability of the financial sector in general.

Therefore, personal data protection should be viewed as part of a strategic long-term investment, not merely as a legal obligation or administrative burden. In an increasingly complex digital era, the success of financial institutions depends heavily on their ability to maintain the confidentiality and integrity of customer data. Implementing a comprehensive data protection policy, complying with applicable regulations, and strengthening internal governance are essential steps in building sustainable trust.

Investment in data protection also contributes to creating a healthy competitive climate, reducing potential legal and reputational risks, and increasing financial inclusion nationally. With a strong data protection system, the banking sector will be better prepared to face cyber threats and adapt to global standards. Indonesia itself is facing real challenges, where cases of personal data leaks continue to increase, not only in the banking sector but also in e-commerce and fintech. This shows weak information governance in various digital sectors. Failure to protect data not only impacts public trust, but also the sustainability of digital financial businesses in the long term. (Ali et al., 2022)

A real example is seen from the widespread use of mobile banking, e-wallet, and online lending services in people's daily lives. Behind this convenience, there are serious risks that threaten users' personal data. The spread of ID card data, account information on social media, to data misuse by internal elements, shows how fragile data protection is today. Therefore, data protection policies must be part of a sustainable growth strategy. This includes strengthening the security system, increasing the capacity of human resources in the financial sector, and enforcing regulations such as the PDP Law. The benefits are not only in the form of preventing losses, but also in building customer loyalty and a strong reputation for financial institutions.

Concrete steps are needed from all stakeholders, including OJK, BI, and Kominfo, to oversee the effectiveness of this policy. Regulation alone is not enough, there must be institutional commitment and synergy between institutions. Because in the end, a safe and sustainable digital financial industry can only grow on the foundation of public trust, one of the determinants of which is how customer personal data is managed and protected. Based on this, this article raises two main issues, namely: how the concept of personal data protection is applied in digital banking, and what is the urgency of legal protection for customer data in the current digital financial ecosystem.

## 2. METHODS

The research method used is normative juridical. Normative juridical legal research is conducted by examining primary and secondary legal materials relevant to the object of study. This research is descriptive-analytical, which aims to systematically describe how the concept of personal data protection is applied in digital banking, and what is the urgency of legal protection for customer data. (Mahmud, 2005) According to Soerjono Soekanto, Normative legal research consists of: legal principles; legal systematics; Research on the level of legal synchronization; on legal history; comparative law. This normative legal research uses the following approaches: Statute Approach, Conceptual Approach, Case Approach. The technique of collecting legal materials is carried out through library research, namely by collecting and reviewing various legal literature, laws and regulations, court decisions, and relevant policy documents. (Sukanto, 2009)

## 3. FINDINGS AND DISCUSSION

### The Concept of Customer Personal Data Protection in Digital Banking

In the era of increasingly massive digital transformation, the concept of personal data protection

has become a main pillar in the digital banking ecosystem in Indonesia. As the adoption of digital financial services such as mobile banking, internet banking, and application-based financial platforms increases, customers' personal data ranging from identity, account numbers, to transaction history have become very valuable and vulnerable objects. Therefore, the implementation of personal data protection cannot be seen as a complementary aspect, but must be an integral part of the banking management and service system. (Prayogo et al., 2024)

In Indonesia, the implementation of the concept of personal data protection in the digital banking sector has received legal legitimacy through Law Number 27 of 2022 concerning Personal Data Protection (UU PDP). This regulation requires every institution, including banks, to manage personal data in a transparent, limited, and accountable manner. In addition, OJK and Bank Indonesia regulations also emphasize the obligation of financial institutions to ensure the security of information systems and prevent data leaks that can harm customers. (Soana, 2024).

However, in its implementation, the application of this concept still faces various serious challenges. Cases of customer personal data leaks still often occur, both through cyber attacks from external parties and data misuse by internal parties. This shows the still weak internal supervision, lack of human resource capacity, and the incomplete development of a data protection culture within the banking institution itself.

In addition, many customers still do not understand their rights over personal data submitted to the bank. This is a separate obstacle in encouraging transparency and accountability of banking institutions. In fact, in international practice, personal data protection is not only an obligation of service providers, but also an active right of consumers to control, know, and access information about how their data is used.

Thus, the implementation of the concept of personal data protection in digital banking in Indonesia must be directed at a comprehensive approach, including strengthening regulations, modernizing digital security infrastructure, increasing public digital literacy, and consistent law enforcement. Only in this way can public trust in the digital financial system be maintained, and Indonesia can realize a safe, inclusive, and sustainable digital banking industry. (Javed, 2021)

To achieve an effective personal data protection system in the digital banking sector, a holistic and cross-sectoral approach is needed, not only relying on declarative legal norms, but also on technical implementation, institutional culture, and community participation as data owners. There are four main elements that are interrelated and mutually reinforcing:

a. Comprehensive Regulatory Strengthening

Although Indonesia has passed Law Number 27 of 2022 concerning Personal Data Protection (UU PDP), strong implementation requires detailed implementing regulations, as well as harmonization with sectoral regulations such as POJK No. 6/POJK.07/2022 and Bank Indonesia Regulation No. 23/6/PBI/2021. It is also important to clarify the roles and authorities between institutions, such as OJK, BI, and Kominfo, so that there is no overlap or lack of supervision. In addition, administrative and criminal sanction mechanisms need to be strictly enforced against violations, to provide a deterrent effect and build compliance. (Mahameru et al., 2023)

b. Modernizing Digital Security Infrastructure

Digital transformation in the banking sector must be accompanied by increased information technology capacity. Banks and digital financial institutions are required to implement cybersecurity systems based on international standards, such as ISO/IEC 27001. Technologies such as data encryption, multi-factor authentication, adaptive firewalls, and intrusion detection systems

(IDS) must be the minimum standard. In addition, periodic testing through system security audits (penetration tests) is needed to map vulnerabilities and fix security gaps.

c. Increasing Digital Literacy and Public Awareness

Indonesian people's digital literacy is still relatively low, especially regarding awareness of the importance of protecting personal data and understanding their rights. Many customers are unaware that their data can be misused, or are unaware of the complaint procedure if their data is leaked. Therefore, banks must be proactive in providing education to customers, including providing clear, easily accessible, and transparent privacy policies. Digital literacy programs must also be part of national public policy involving educational institutions, media, and other digital platforms. That way, people will not only become users, but also protectors of their own personal data.

d. Consistent and Transparent Law Enforcement

Law enforcement for personal data breaches remains a challenge in Indonesia. Many data breach cases are not fully investigated, or only end with administrative warnings. In fact, for the concept of personal data protection to be meaningful, there must be guarantees of justice and accountability. Strict and transparent law enforcement, including digital forensic investigations and public involvement, will strengthen the credibility of data protection policies.

Law Number 27 of 2022 together with POJK Number 6/POJK.07/2022 strictly regulates the rights and responsibilities of each party involved in managing personal data. The following are some of the customer rights related to personal data protection in digital banking services: (Tasman & Ulfanora, 2023)

1. Right to personal data security

Customers have the right to a guarantee of the security of their personal data obtained by the bank in the context of providing digital services. This information must be protected from all forms of illegal access or misuse. In this case, the bank is responsible for implementing an adequate information security system, including data encryption technology and multi-factor authentication as technical protection measures. This provision is in line with the mandate in Article 6 and Article 21 of OJK Regulation No. 12/POJK.07/2022, which regulates the protection of financial service consumers.

2. Right to information and transparency

Every customer has the right to obtain accurate and transparent information regarding the entire process of managing their personal data—from the collection, storage, processing, to the utilization of data in the digital service system. Banks are required to convey privacy policies openly and explain the customer's rights to provide or refuse approval for the use of their data. This right is explicitly regulated in Article 26 of the Regulation of the Minister of Communication and Informatics (Permenkominfo) No. 20 of 2016.

3. Right to lodge a complaint

If there is an alleged violation of privacy or management of customer personal data, then the customer has the right to submit an official complaint. The complaint mechanism can be submitted to the bank or to the Financial Services Authority (OJK), with the aim of obtaining a fair and transparent resolution. The regulation regarding this right is stated in Article 29 paragraph (1) and (2) of Permenkominfo No. 20 of 2016.

4. Right to data erasure

Customers have the right to submit a request for deletion of their personal data, especially if the

data is no longer relevant, no longer needed, or its use is contrary to applicable laws or privacy policies. The Bank is obliged to process this request within the time period specified in the regulation. This provision is regulated in Article 25 paragraph (1) letter b of Permenkominfo No. 20 of 2016.

#### 5. Right to withdraw consent

Customers also have the right to withdraw their consent to the processing or use of personal data by the bank in digital services. Once consent is withdrawn, the bank is required to stop using the data, unless there is a legal basis that requires the processing to continue. This right guarantees customers full control over their personal information, and is part of the principle of legitimate consent-based data protection.

Based on the above, customers are given the right to access, update, or delete their personal data in accordance with applicable provisions, thus providing greater control over the personal information they have. This allows customers to ensure that the data stored in banking institutions remains accurate and relevant. Meanwhile, banks have a responsibility to convey information openly regarding the management of customers' personal data and ensure the security of the data. This responsibility includes implementing strict procedures in the process of collecting, storing, and utilizing personal data to prevent potential misuse.

Provisions regarding sanctions for violations of personal data protection are also explicitly stated in Law Number 27 of 2022 and POJK Number 6/POJK.07/2022. These two regulations provide a legal basis for the application of various forms of sanctions against banking institutions that do not comply with data protection regulations. The types of sanctions that can be imposed include administrative fines, temporary to permanent suspension of the institution's activities, and other legal actions according to the level of violation. The main purpose of imposing these sanctions is to create a deterrent effect, strengthen the institution's compliance with regulations, and provide maximum protection for customers from the risk of misuse of personal data. Thus, these sanctions also function as a supervisory mechanism so that banking institutions carry out data management professionally and responsibly.

The issue of personal data protection in the digital banking world is no longer just a technical matter, but has become a strategic issue in maintaining public trust in modern financial services. Amid the increasing use of digital banking platforms in Indonesia, threats to customer privacy and data security are issues that cannot be ignored. As a form of state commitment, the government has enacted Law Number 27 of 2022 concerning Personal Data Protection (UU PDP), and strengthened it with sectoral regulations such as POJK No. 6/POJK.07/2022 which regulates the protection of financial service consumers. This regulation explicitly stipulates the rights and obligations between customers and financial service providers in the context of personal data management.

However, the effectiveness of data protection policies is not enough if it only relies on the national legal framework. Indonesia needs to integrate global standards into data protection practices, as has been implemented through the General Data Protection Regulation (GDPR) in the European Union. This harmonization is important, considering that customer personal data now crosses national borders through increasingly complex and globally connected financial technology systems.

The steps to adjust to international practices will not only strengthen legal protection for customers, but also improve the competitive position of financial institutions on a global scale. In the competitive era of digital finance, customer trust is a major asset. Institutions that are able to build a secure and transparent data management system will win market loyalty, while those who are negligent will lose relevance. Thus, aligning national regulations with global standards is not just a

discourse on legal harmonization, but a strategic need to maintain the credibility and sustainability of Indonesia's digital financial industry in the future.

Customer trust is now an invaluable asset in the competitive world of digital finance. Customers' decisions to continue using certain services are highly dependent on their perception of the institution's integrity and responsibility in maintaining the confidentiality of their personal information. Financial institutions that are able to design a data protection system based on the principle of prudence, use the latest security technology, and transparency in information management will gain market trust and loyalty in the long term. On the other hand, negligence in data protection will not only damage the institution's reputation, but can also trigger an exodus of users, lawsuits, and sanctions from regulators.

More than just formal compliance with global standards such as the General Data Protection Regulation (GDPR), regulatory harmonization shows that Indonesia is committed to creating a digital ecosystem that is safe, fair, and trustworthy for investors, international partners, and the public. This is important, considering that cross-border data flows have become an integral part of the modern financial system, and Indonesian financial institutions need to demonstrate that they have the capacity to manage complex global risks.

Thus, aligning national policies with international practices is not merely a discourse on legal harmonization, but is part of a strategic effort to strengthen institutional credibility, maintain the stability of the national digital financial system, and ensure the sustainability of the growth of the Indonesian financial sector in a dynamic and challenging global landscape.

### **The Urgency of Legal Protection for Customer Data in the Digital Financial Ecosystem**

The development of information technology has revolutionized the financial services industry globally, including in Indonesia. Digital banking, fintech, e-wallet, and various forms of application-based financial services have become the main choices for modern society in accessing financial products and services. However, this convenience brings increasingly complex legal and ethical consequences, especially in terms of managing and protecting customer personal data. (Kusuma & Asmoro, 2021)

In the digital financial ecosystem, customer data is a very vital asset. This data includes not only identity information, but also consumption patterns, transaction preferences, and the user's geographic location. The data collected, processed, and stored by these financial institutions is very vulnerable to misuse if not regulated and protected by law.

The urgency of legal protection for customer data arises from several crucial aspects, including: (Lutfi et al., 2024)

- a. First, personal data is part of the right to privacy guaranteed in the constitution and human rights principles. Therefore, the state has a responsibility to provide strong legal guarantees so that these rights are not violated, especially by business actors in the financial sector.
- b. Second, in practice, many cases of data leaks and misuse occur due to weak governance and internal supervision of financial institutions. Without strict legal regulations and effective enforcement mechanisms, customers are in a very vulnerable position. In some cases, customer data is sold to third parties without permission, or used to offer products that do not meet needs.
- c. Third, public trust in digital financial institutions is highly dependent on the extent to which personal data protection is legally enforced. When customers feel safe and confident that their data is managed responsibly, the level of participation in the digital financial system will increase. Conversely, legal uncertainty can trigger distrust, even drawing people back to the conventional

financial system.

- d. Fourth, this urgency is also related to national competitiveness in the global arena. Countries that have a strong data protection legal framework, as seen in the implementation of the General Data Protection Regulation (GDPR) in the European Union, tend to be more trusted in cross-border digital transactions. Therefore, Indonesia needs to strengthen its legal system so that the national digital financial ecosystem is not left behind competitively.

In response to this challenge, the presence of Law Number 27 of 2022 concerning Personal Data Protection is an important step in building a stronger legal foundation for data protection. However, the implementation of this regulation still faces major challenges, such as the lack of an independent data protection authority, low digital legal literacy in the community, and less than optimal sanctions for violations.

The enactment of Law Number 27 of 2022 concerning Personal Data Protection (UU PDP) marks an important step in the development of a comprehensive national legal framework for personal data protection, including in the digital financial sector. This law provides a normative basis for accountable, transparent, and fair data processing, and recognizes the rights of data subjects as part of human rights guaranteed by the constitution. In the context of technology-based banking and financial services, the existence of the PDP Law is very relevant considering the high intensity of customer data processing by financial institutions.

However, the implementation of this law in the field still faces a number of structural and substantial obstacles. One of the most fundamental challenges is the lack of an independent personal data protection authority, as mandated in the transitional provisions of the PDP Law. The absence of this institution means that the functions of monitoring and enforcing the law against data violations are still spread across various agencies, which ultimately has implications for weak coordination and a suboptimal enforcement process.

In addition to institutional issues, the low level of digital legal literacy in society is also a serious obstacle in encouraging the effective implementation of this law. Most customers who use digital financial services do not yet understand their rights to personal data, including the right to know, access, correct, and delete data collected by service providers. This condition causes many violations of privacy to go unreported or not followed up legally, due to the lack of awareness and understanding of the law at the user level.

On the other hand, there is still an imbalance in the application of administrative and criminal sanctions for data protection violations. In some cases, financial institutions that are proven to be negligent or misuse customer data are only given light administrative warnings, without adequate legal consequences. This has an impact on the low deterrent effect and creates a negative precedent that violations of personal data are not serious violations in the eyes of the law.

Thus, the success of the implementation of the PDP Law is not only determined by the normative substance of the law, but is also greatly influenced by institutional readiness, supervisory capacity, and the level of digital literacy of the community. For this, strategic steps are needed, including:

1. Accelerating the establishment of an independent and professional data protection authority.
2. Strengthening synergy between financial sector regulators such as OJK and BI with data supervisory institutions.
3. Integration of privacy by design principles into the operational systems of financial institutions.
4. Improving data literacy and privacy programs for customers.
5. Enforcement of fair and proportionate sanctions for personal data breaches.

Thus, legal protection of customer data is not only normative, but also strategic. This concerns the future of financial inclusion, cybersecurity, and the sustainability of the digital financial industry itself. Synergy is needed between regulators, financial service providers, and the public to ensure that customer rights to personal data are truly protected in practice, not just on paper.

#### 4. CONCLUSION

Protection of customer personal data is a key element in creating public trust and ensuring the sustainability of the digital financial sector in Indonesia. Amidst the increasingly rapid flow of digital transformation and the increasing use of technology-based banking services, customer personal information has become a vital component that demands strong, responsible, and sustainable legal protection. Currently, personal data protection can no longer be positioned as an operational complement, but must be part of the core strategy in the governance of financial institutions. The presence Law Number 27 of 2022 concerning Personal Data Protection and POJK No. 6/POJK.07/2022 provide a legal basis that recognizes customers' rights to access, correct, or delete their personal data. Both regulations also require financial institutions to ensure the security of customer data and manage information transparently. However, the effectiveness of implementing these regulations still faces serious obstacles. Among them are the lack of an independent supervisory body that has full authority to oversee the implementation of the PDP Law, low awareness of digital law among the public, and the less than optimal imposition of sanctions for personal data violations. On the other hand, the continued misuse of data by internal and external parties indicates a weak supervisory system and the lack of a strong data protection culture within the financial institution environment.

#### REFERENCES

- Ali, A., Fahminuddin, M., & Hidayatullah, S. (2022). Islamic Technology Finance and Digital Banking. *Zhafir: Journal of Islamic ...*, 4(1), 47–60.  
<https://jurnalsains.id/index.php/zhafir/article/view/137%0Ahttps://jurnalsains.id/index.php/zhafir/article/download/137/109>
- Denisyana, NP, Budiarta, INP, & Putra, IMAM (2024). Legal Protection of Customer Personal Data by Banks in Transactions Through Internet Banking. *Journal of Legal Preferences*, 5(2), 246–252.  
<https://doi.org/10.22225/jph.5.2.8088.246-252>
- Iqbal, J., Soroya, SH, & Mahmood, K. (2024). Financial information security behavior in online banking. *Computers & Security*. Advance online publication. <https://doi.org/10.1177/02666669221149346>
- Javed, Y., Al Qahtani, E., & Shehab, M. (2021). Privacy policy analysis of banks and mobile money services in the Middle East. *Future Internet*, 13(1), 10. <https://doi.org/10.3390/fi13010010>
- Jagadish, R. (2024). Data encryption and privacy in cloud banking: best practices and regulatory compliance. *International Research Journal of Modernization in Engineering Technology and Science*, 6(4), 8139–8145. <https://doi.org/10.56726/IRJMET53838>
- Kusuma, H., & Asmoro, WK (2021). Development of Financial Technology (Fintech) Based on Islamic Economic Perspective. *ISTITHMAR: Journal of Islamic Economic Development*, 4(2), 141–163.  
<https://doi.org/10.30762/itr.v4i2.3044>
- Lutfi, MP, Kurniasari, E., & Putri, FEA (2024). The Urgency of Legal Protection for Bank Customer Privacy Data in the Era of Digital Development. *Multidisciplinary Journal of Academic Sciences*, 1(5), 210–218. <https://doi.org/10.61722/jmia.v1i5.2679>
- Mahameru, DE, Nurhalizah, A., Wildan, A., Haikal Badjeber, M., & Rahmadia, MH (2023). Implementation of the Personal Data Protection Law on the Security of Identity Information in Indonesia. *Jurnal Esensi Hukum*, 5(2), 115–131.  
<https://journal.upnvj.ac.id/index.php/esensihukum/index>



- Mahmud, P. (2005). Legal Research. Kencana Prenada Media Group.
- Maisah, Sari, SP, Sudiarni, & Ompusunggu, HP (2023). Legal Analysis of Customer Personal Data Protection in Digital Banking Services in Indonesia. *Aufklarung: Jurnal Pendidikan*, 3(3), 285–290.
- Prayogo, P., Korah, RS., Soepeno, MH, & Kasenda, V. (2024). Analysis of Legal Protection of Customer Personal Data in Internet Banking Transactions in North Sulawesi. *Academic Nuances: Journal of Community Development*, 9(1), 39–54. <https://doi.org/10.47200/jnajpm.v9i4.2089>
- Sukanto, S. and SM (2009). Normative Legal Research: A Brief Review. PT Raja Grafindo Persada.
- Soana, G., & de Arruda, T. (2024). Central Bank Digital Currencies and financial integrity: finding a new trade-off between privacy and traceability within a changing financial architecture. *Journal of Banking Regulation*, 25(4), 467–486.
- Tasman, T., & Ulfanora, U. (2023). Legal Protection for Digital Bank Customers. *UNES Law Review*, 6(1), 1624–1635. <https://doi.org/10.31933/unesrev.v6i1.962>

