JLPH: Journal of Law, Politic and Humanities
E-ISSN: 2962-2816
P-ISSN: 2747-1985
https://dinastires.org/JLPH dinasti.info@gmail.com +62 811 7404 455
DOI: https://doi.org/10.38035/jlph.v5i5

The Legal Protection of Debtors as Victims of Personal Data Misuse in the Use of Shopee PayLater Service

Leksi[1], Tahasak Sahay[2], Vicka Prama Wulandari[3].
[1]Universitas Palangka Raya, Central Kalimantan, Indonesia, exoelleksi@gmail.com.
[2]Universitas Palangka Raya, Central Kalimantan, Indonesia, tahasak@law.upr.ac.id..
[3]Universitas Palangka Raya, Central Kalimantan, Indonesia, vickapramawulandari@gmail.com.

Corresponding Author: exoelleksi@gmail.com[1]

Abstract: Shopee PayLater services offer convenience in transactions but also pose risks of personal data misuse, thereby underscoring the importance of legal protection under the Electronic Information and Transactions Law (ITE Law) and the Personal Data Protection Law (PDP Law) to maintain consumer trust. Shopee PayLater facilitates transactions through a "buy now, pay later" system; however, it also exposes debtors to potential misuse of personal data. This study examines the legal protection afforded to Shopee PayLater debtors against the misuse of personal data in Indonesia, focusing on the effectiveness of regulatory frameworks and the legal responsibility of Shopee PayLater as a data controller. A normative juridical approach is employed to analyze the Electronic Information and Transactions Law, the Consumer Protection Law, and the Personal Data Protection Law. The findings reveal that, although a solid legal foundation exists, the implementation of data protection remains suboptimal due to weaknesses in cybersecurity systems and unethical debt collection practices. These gaps hinder effective protection for debtors. The researcher recommends enhanced investment in data security, improvement of privacy policy transparency, and stricter government oversight to ensure regulatory compliance and stronger consumer protection.

Keyword: Legal Protection, Personal Data, Shopee PayLater.

INTRODUCTION

In the increasingly advanced digital era, innovations in the financial services sector—particularly in the form of financial technology (fintech)—have brought significant convenience to consumers. One of the most popular innovations today is the "Buy Now, Pay Later" (BNPL) service, such as that offered by Shopee PayLater (Muzdalifa et al, 2018). This service enables consumers to conduct purchase transactions with deferred payments, thereby providing financial flexibility. Nevertheless, behind such convenience lies a risk that cannot be overlooked—namely, the potential misuse of users' personal data. The personal data submitted by debtors, including identity information, financial history, and other sensitive data, is vulnerable to misuse by irresponsible parties (Nasutian, 2020). Such misuse may take the form

of unauthorized access, hacking, or use of data for fraudulent purposes, ultimately causing both financial and emotional harm to consumers.

The importance of legal protection in the digital economy cannot be underestimated, especially in maintaining consumer trust in the rapidly growing fintech services in Indonesia. Personal data is often referred to as the "new oil" of the digital age, indicating its immense value and high potential for exploitation. Without adequate regulation, the risk of data misuse may compromise the integrity of the digital financial system and harm multiple stakeholders (Kelibia et al, 2025). Legal protection serves not only as a tool to provide remedies to victims but also as a deterrent mechanism for business actors who might otherwise neglect data security obligations. In the context of Shopee PayLater, where users' financial and personal data constitute highly valuable assets, the existence of a clear and firm legal framework becomes essential. It ensures that consumers' rights to feel secure and protected in transactions are upheld, while also encouraging business actors to assume responsibility for data governance.

Indonesia has taken several steps in developing a legal framework to protect personal data, particularly through the Electronic Information and Transactions Law (ITE Law) and the Personal Data Protection Law (PDP Law). The ITE Law, enacted in 2008 and amended in 2016, regulates various aspects of electronic transactions, including provisions on the protection of personal data. However, the enactment of the Personal Data Protection Law in 2022 marks a significant milestone, as it specifically governs the protection of personal data in both public and private sectors. This law sets out the rights of data subjects, the obligations of data controllers and processors, as well as sanctions for violations (Pradana & Saragih, 2024). For users of Shopee PayLater, this legislation guarantees that their data must be processed lawfully, transparently, and with their explicit consent.

Fintech companies such as Shopee are categorized as data controllers and processors, which imposes upon them legal obligations to protect users' personal data. Pursuant to the Personal Data Protection Law, companies are required to implement adequate security measures to prevent data breaches, ensure that data is collected and processed only with explicit consent, and provide users with access to correct or erase their data (Supriyanti, 2023). In the event of a data breach, companies are obligated to promptly notify both the competent authority and the affected users. Any violation of these obligations may result in severe sanctions, including administrative fines, restrictions on business operations, or even criminal liability.

In situations where personal data is misused within the Shopee PayLater ecosystem, Indonesian law provides several avenues for victims to seek legal redress. Under the Personal Data Protection Law, victims may file a complaint with the relevant supervisory authority, which shall conduct an investigation and impose appropriate sanctions on the offending party (Rivaldo & Syailendra, 2024). Victims may also initiate civil proceedings to claim compensation for damages suffered as a result of the misuse of their data. The law further obligates companies such as Shopee to fully cooperate in such investigations and to take immediate remedial measures, including the provision of compensation to affected users. The Electronic Information and Transactions Law (ITE Law) provides criminal sanctions for serious data misuse cases, such as identity theft or fraud, thereby affording consumers an additional layer of legal protection. For Shopee PayLater debtors, these legal provisions are essential to ensure that their rights are safeguarded and that they are not left vulnerable to data-related offenses.

The legal issues addressed in this research concern the effectiveness of the Indonesian regulatory framework in protecting individuals whose personal data has been misused within the Shopee PayLater service, as well as the extent to which Shopee PayLater has fulfilled its legal obligations as a data controller. Specifically, this study examines whether the existing laws and regulations in Indonesia provide sufficient and effective legal protection for victims of personal data misuse in the context of digital financial services. Furthermore, it explores the degree to which Shopee PayLater has implemented appropriate measures, in accordance with

the Personal Data Protection Law, to prevent the unauthorized use or exploitation of debtors' personal data and to uphold its responsibilities in safeguarding consumer rights.

METHOD

This research employs a normative juridical approach (Ali, 2024), to analyze the legal protection against the misuse of personal data belonging to Shopee PayLater debtors, with a particular focus on the applicable laws and regulations in Indonesia, including the Law on Electronic Information and Transactions (ITE Law), the Consumer Protection Law, and the Personal Data Protection Law (PDP Law).

This approach involves a thorough examination of legal provisions concerning financial technology (fintech) and consumer protection, identifying potential weaknesses or gaps within the regulatory framework, and evaluating the effectiveness of the existing legal mechanisms in safeguarding users' rights and ensuring data security. The research method includes legal interpretation, statutory analysis, and conceptual analysis, supported by a literature review of relevant legal doctrines and expert opinions to provide a comprehensive understanding of how legal norms are applied and enforced in practice.

RESULTS AND DISCUSSION

Definition and Types of Personal Data

By definition, personal data refers to any form of information that can be used to identify an individual, either directly or indirectly (Suharyanti & Sutrisni, 2021). In the advancing digital era, personal data has become highly valuable as it can be utilized for various purposes, ranging from service personalization to consumer behavior analysis. This information may include simple details such as name, address, and telephone number, to more complex data such as health records or political preferences. The significance of personal data lies in its impact on an individual's life; for example, financial information can affect a person's access to credit, while location data can reveal daily life patterns (Priliasari, 2023). Personal data is generally categorized into two main types: general personal data and sensitive personal data. General personal data encompasses information that can identify an individual but does not necessarily have a significant impact if misused. This type of data is typically more accessible and often serves as the starting point for entities seeking to build user profiles.

Sensitive personal data, by definition, consists of information that has the potential to cause substantial harm to an individual if it falls into the wrong hands (Disemadi et al, 2023). This category includes national identification numbers (such as the NIK in Indonesia), financial information such as bank account numbers or credit history, health data including medical records, as well as highly private details such as sexual orientation or religious beliefs. Sensitive data is often the primary target in data breaches due to its high value, both for commercial interests and criminal purposes. In Indonesia, sensitive data receives special attention under the law because its misuse may result in discrimination, identity theft, or significant financial harm to individuals.

Legal Protection of Personal Data in Indonesia

Legal protection of personal data in Indonesia has evolved in line with the growing awareness of the importance of privacy in today's digital era. A major milestone in this development is the enactment of Law Number 27 of 2022 concerning Personal Data Protection (PDP Law), which stands as the first regulation specifically and comprehensively governing the protection of personal data in the country (Kusuma, 2023). The Personal Data Protection Law defines personal data as information that can identify an individual, whether through electronic or non-electronic systems, encompassing both general and sensitive data. This law was enacted in response to the increasing number of data breaches and the misuse of personal information, particularly within the technology and digital finance sectors.

The Personal Data Protection Law grants several fundamental rights to data subjects—individuals whose personal data is processed. These rights include the right to be informed of the purpose of data collection, the right to access their personal data, the right to rectify inaccurate data, and the right to request the erasure of data that is no longer relevant. Furthermore, individuals have the right to withdraw their consent to the use of personal data, thereby affording them greater control over the information they choose to share.

The PDP Law also imposes obligations on data controllers and data processors, i.e., entities responsible for the management of personal data. A data controller, who determines the purposes and means of processing, is required to ensure that data is collected lawfully, based on clear consent, and used solely for the agreed purposes (Mahameru et al, 2023). They are also mandated to implement appropriate security measures to prevent unauthorized disclosure, alteration, or deletion of data. Meanwhile, a data processor, who processes data on behalf of the controller, is similarly obligated to maintain the confidentiality and integrity of the information. Violations of these obligations may result in administrative sanctions or criminal penalties, depending on the severity of the breach. Legal protection of personal data in Indonesia is further supported by other relevant legislation, such as Law Number 11 of 2008 concerning Electronic Information and Transactions (ITE Law), as amended in 2016.

Misuse of Personal Data in Digital Lending Services

Digital lending services such as Shopee PayLater have become a popular solution for many individuals in Indonesia to meet their financial needs quickly and conveniently. However, behind this convenience lies a significant risk of personal data misuse (Nugrahanti et al, 2024). In this context, misuse of personal data refers to the utilization of user information without lawful consent or for purposes that exceed the scope of the service.

One common practice is the excessive collection of data, whereby applications request access to information irrelevant to the lending process, such as contact lists, location data, or message history. Non-transparent data sharing is another prevalent form of misuse in digital lending services. Many fintech companies collaborate with business partners or affiliates, and user data is frequently shared with third parties without the data subject's explicit consent. This can result in personal information being used to construct highly detailed consumer profiles, which may then be exploited for targeted advertising or even discriminatory pricing practices.

Data breaches due to security violations also constitute a recurring threat in the digital lending industry (Antoine et al, 2025). Although companies are legally obligated to implement adequate security systems, cyberattacks or technical errors—such as poor server configuration—can lead to the exposure of millions of user records. In the context of Shopee PayLater, such data breaches could involve sensitive information such as credit card numbers, transaction history, or personal identification details.

The consequences may be far-reaching, ranging from direct financial loss to irreparable reputational damage. These incidents underscore the fact that even major companies are not immune to data security risks. Furthermore, data misuse is often observed in unethical debt collection practices, which have become a major concern in the realm of digital lending services. Some companies have been known to use personal data, such as users' contact lists, to reach out to their family members or friends as part of their debt collection strategy, thereby infringing upon the privacy rights of both the debtor and third parties.

Effectiveness of Legal Protection in Shopee PayLater Services

The misuse of debtors' personal data in Shopee PayLater services has become an increasingly prominent issue in line with the growing use of digital platforms for financial transactions. This issue not only threatens individual privacy but also results in both material and non-material harm to debtors. In Indonesia, three principal laws serve as the legal framework for addressing such cases: Law Number 27 of 2022 concerning Personal Data

Protection (PDP Law), Law Number 1 of 2024 as the Second Amendment to Law Number 11 of 2008 on Electronic Information and Transactions (EIT Law), and Law Number 8 of 1999 on Consumer Protection (CPL Law).

The Personal Data Protection Law (PDP Law) provides a clear definition of personal data as any information that can be used to identify an individual, either directly or indirectly (Indonesia, 2022). In the context of Shopee PayLater, a debtor's personal data includes information such as full name, phone number, address, and financial history related to payment activities. Article 4 of the PDP Law categorizes personal data into two main types: specific personal data and general personal data. Financial data, which is central to Shopee PayLater services, falls under the category of specific data that requires a higher level of protection due to its sensitive nature. This provision underscores that debtors' data must not be treated carelessly and must be protected by stringent security standards to prevent unauthorized misuse.

The PDP Law not only defines personal data but also grants crucial rights to data subjects, in this case, Shopee PayLater debtors. Pursuant to Article 5, debtors have the right to be informed transparently regarding how their personal data is collected, used, and managed by the data controller. Furthermore, Article 8 grants debtors the right to request the deletion of their personal data from the system when it is no longer necessary or when a violation has occurred. Article 12 of the PDP Law entitles debtors to file legal claims and seek compensation in the event of data misuse. These rights serve as essential tools for debtors to assert control over their personal information and to seek redress for harmful conduct, thereby reinforcing their position in responding to personal data violations (Arhansyah et al, 2024).

In conclusion, it may be asserted that legal protection for victims of personal data misuse in Shopee PayLater services in Indonesia is firmly established through Law Number 27 of 2022 concerning Personal Data Protection (PDP Law), the Electronic Information and Transactions Law (EIT Law), and the Consumer Protection Law (CPL Law), which collectively regulate the rights of debtors to control their data, claim compensation, and seek justice through legal mechanisms such as civil lawsuits or complaints to competent authorities.

Legal Responsibility of Shopee PayLater as Data Controller

As a fintech corporate entity, the processing of personal data by Shopee PayLater as a data controller must comply with the principles stipulated in Article 16 of the Personal Data Protection Law (PDP Law). These principles include limiting data collection to specific needs, conducting data processing lawfully in accordance with applicable laws, and ensuring transparency to the data subject. In other words, debtor data may only be collected for agreed purposes, such as credit processing or identity verification, and must not be used beyond that context without consent. Furthermore, such data must be protected against threats like hacking or unauthorized access. Violation of these principles provides debtors with a strong legal basis to hold negligent parties accountable, thereby fostering a more responsible and secure data processing system.

Shopee PayLater has legal obligations under the PDP Law to ensure the security of debtor data. Article 20 mandates a clear legal basis for each data processing activity, such as written consent or contracts agreed upon by the debtor. Article 36 emphasizes that the data controller must maintain the confidentiality of the information they manage and prevent leakage or misuse by third parties. Additionally, Article 46 of the PDP Law requires immediate notification to debtors in the event of data protection failure, such as hacking or security breaches. These obligations place significant responsibility on Shopee PayLater not only to collect data ethically but also to safeguard it with adequate security measures.

The PDP Law provides strict sanctions. Article 65 explicitly prohibits unlawful collection, disclosure, or use of personal data, subjecting violators to criminal penalties including imprisonment and substantial fines. Meanwhile, Article 67 regulates various criminal sanctions depending on the type of violation, such as data misuse for extortion or fraud. These

sanctions are intended not only to punish offenders but also to provide assurance to debtors that the law supports them in combating detrimental actions. With these provisions, Shopee PayLater debtors are guaranteed that perpetrators of data misuse can be legally prosecuted (Putri, 2021).

The Electronic Information and Transactions Law (EIT Law) also offers additional protection for Shopee PayLater debtors. Article 27 of the EIT Law prohibits the dissemination of electronic information that violates decency, which may include the misuse of personal data for indecent purposes. Article 27B forbids threats or extortion carried out by exploiting electronic data, while Article 28 prohibits the spread of false information that harms consumers in digital transactions. Violations of these provisions are subject to criminal sanctions as set forth in Articles 45 and 45A, which include imprisonment and fines. This protection is particularly relevant given the frequent occurrence of data misuse in the digital realm, making the EIT Law an important complement within the legal framework.

The Consumer Protection Law (CPL Law) further strengthens the position of debtors as consumers of Shopee PayLater services. Article 4 guarantees consumers the right to security, comfort, and truthful and clear information regarding the services they use. Article 7 obliges business actors, including Shopee PayLater, to provide accurate information and bear responsibility for losses arising from their negligence. In cases of data misuse causing harm to debtors, Articles 19 and 23 enable them to claim compensation through legal channels. These provisions ensure that debtors are protected not only as data subjects but also as consumers entitled to fair and safe services (Faris & Winario, 2024).

The CPL Law also provides dispute resolution mechanisms available to Shopee PayLater debtors. Article 45 allows debtors to file claims against business actors through consumer dispute resolution bodies or directly in court. If the business actor is proven to have violated consumer protection obligations, Article 62 prescribes criminal sanctions such as fines or imprisonment. This mechanism offers a clear pathway for debtors to seek justice, especially when personal data misuse cannot be resolved amicably with Shopee PayLater.

However, these responsibilities have yet to be fully implemented, as evidenced by ongoing cases of data breaches and unethical collection practices involving misuse of personal information, such as contacting debtors' family or friends. This indicates weaknesses in cybersecurity systems and adherence to transparency principles. While measures such as encryption and authentication have been applied, they remain insufficient to prevent cyber threats or data misuse by third parties. Therefore, Shopee PayLater needs to enhance investments in security, clarify privacy policies to users, and ensure that data is only used for agreed purposes to comply with standards and prevent further harm to debtors.

CONCLUSION

Legal protection for victims of personal data misuse involving Shopee PayLater debtors in Indonesia is firmly grounded in the Personal Data Protection Law (PDP Law), the Electronic Information and Transactions Law (EIT Law), and the Consumer Protection Law (CPL Law). Collectively, these regulations grant debtors the rights to control their personal data, claim compensation, and seek justice through legal mechanisms such as civil lawsuits or complaints to regulatory authorities.

However, the effectiveness of these protections is hindered by implementation weaknesses, including incidents of data breaches and unethical debt collection practices, which indicate that Shopee PayLater has not fully complied with its obligations as a data controller, particularly in maintaining cybersecurity and transparency in data management. To enhance the protection of Shopee PayLater debtors' personal data, the company must strengthen its cybersecurity system by investing in advanced encryption and authentication technologies, as well as ensure adherence to transparency principles by clearly communicating privacy policies to users. Shopee PayLater should limit data collection strictly to information relevant to its

services, cease unethical debt collection practices, and prohibit data sharing with third parties without explicit consent. Additionally, the government needs to tighten supervision over fintech compliance with the PDP Law and provide consumer education regarding their rights, thereby preserving trust in digital services and minimizing the risk of data misuse.

REFERENCE

Ali, Z. (2021). Metode penelitian hukum. Sinar Grafika.

Arhansyah, R. J., Firmansyah, H., Anhar, I. A., Pribadi, M. F., & Yulianto, Z. H. (2024). Perlindungan Hukum bagi Kreditur dalam Kontrak yang Melibatkan Jaminan Fidusia. Mahalini: Journal of Business Law, 1(1).

Disemadi, H. S., Sudirman, L., Girsang, J., & Aninda, A. M. (2023). Perlindungan Data Pribadi di Era Digital: Mengapa Kita Perlu Peduli? Sang Sewagati Journal, 1(2), 66–90.

Faris, N., & Winario, M. (2024). Perlindungan Konsumen Dalam Perbankan Syariah: Perspektif Hukum Ekonomi Syariah. Multidisciplinary Journal Of Religion And Social Sciences, 1(1), 29–39.

Kelibia, M. U., Dwiputro, L. F., Deniyanto, Y., Anugrah, A. P., & Supriadi, B. (2025). Tinjauan Yuridis Terhadap Regulasi Cryptocurrency Dalam Perspektif Hukum Ekonomi Syariah. Jurnal Kolaboratif Sains, 8(1).

Mahameru, D. E., Nurhalizah, A., Badjeber, H., Wildan, A., & Rahmadia, H. (2023). Implementasi UU perlindungan data pribadi terhadap keamanan informasi identitas di Indonesia. Jurnal Esensi Hukum, 5(2), 115–131.

Muzdalifa, I., Rahma, I. A., Novalia, B. G., & Rafsanjani, H. (2018). Peran fintech dalam meningkatkan keuangan inklusif pada UMKM di Indonesia (pendekatan keuangan syariah). Jurnal Masharif Al-Syariah: Jurnal Ekonomi Dan Perbankan Syariah, 3(1), 1–24.

Nasution, T. H. (2020). Perlindungan Hukum Data Pribadi Nasabah dalam Penggunaan Big Data Oleh Perbankan di Indonesia (Studi Komparatif Penggunaan Data Pribadi Nasabah di Uni Eropa).

Nugrahanti, Y. W., Rita, M. R., Restuti, M. M. D., & Hadiluwarso, M. A. (2024). Perilaku Keuangan Mahasiswa Dalam Penggunaan Paylater: Beli Sekarang-Bayar Nanti. Penerbit NEM.

Pradana, M. A. E., & Saragih, H. (2024). Prinsip Akuntabilitas dalam Undang-Undang Perlindungan Data Pribadi Terhadap GDPR dan Akibat Hukumnya. Innovative: Journal Of Social Science Research, 4(4), 3412–3425.

Priliasari, E. (2023). Perlindungan Data Pribadi Konsumen Dalam Transaksi E-Commerce. Jurnal Rechts Vinding: Media Pembinaan Hukum Nasional, 12(2).

Rivaldo, A., & Syailendra, M. R. (2024). Tanggung Jawab Penyedia Layanan Perbankan Terhadap Penyalahgunaan Data Nasabah Berdasarkan Pasal 46 Ayat 1 UU PDP (Kasus Putusan 615/Pdt. G/2023/Pn Surabaya). UNES Law Review, 6(4), 10658–10665.

Suharyanti, N. P. N., & Sutrisni, N. K. (2021). Urgensi Perlindungan Data Pribadi Dalam Menjamin Hak Privasi Masyarakat. In Prosiding Seminar Nasional Fakultas Hukum Universitas Mahasaraswati Denpasar 2020 (Vol. 1, No. 1, pp. 119–134).

Supriyanti, N. M. (2023). Perlindungan Hukum Atas Kerahasiaan Data Wajib Pajak Dalam Proses Validasi Melalui E-PHTBNotaris/PPAT (Master's thesis, Universitas Islam Sultan Agung (Indonesia)).